University of Pisa

Faculty of Science

Department of Mathematics

PhD Thesis

# Local-Global Divisibility Problems for Elliptic Curves

Advisor:
Prof. R. Dvornicich

PhD Student:
Laura Paladino

2008

*To my mother*
*and to the memory*
*of my father*

# Introduction

In many cases problems concerning number fields can be solved more easily in their completions. By knowing the local solutions, it is often possible to deduce the global ones. Then, in a natural way, many mathematical problems formulated in last century, have in their hypotheses the existence of local solutions everywhere or almost everywhere. A problem of that type is called a *Local-Global Problem*. Some of them were solved successfully. The most famous is the following one:

HASSE PRINCIPLE *Let $F(X_1, ..., X_n) \in k[X_1, ..., X_n]$ be a quadratic form, where $k$ is a number field. Suppose the equation $F = 0$ has a nontrivial solution everywhere locally. Then it has a nontrivial solution in $k$.*

It was proved in 1923-24. Other Local-Global Problems remain open in many cases. In this thesis we shall be concerned mainly with the following question:

PROBLEM *Assume that $k$ is a number field and $\mathcal{A}$ is a commutative algebraic group over $k$. Let $P \in \mathcal{A}(k)$. Denote by $M_k$ the set of the places $v \in k$ and by $k_v$ the completion of $k$ at the valuation $v$. Suppose for all but finitely many $v \in M_k$, there exist $D_v \in \mathcal{A}(k_v)$ such that $P = qD_v$, where $q$ is a positive integer. Is it possible to conclude that there exists $D \in \mathcal{A}(k)$ such that $P = qD$?*

This problem is known as *Local-Global Divisibility Problem*. By using the Bézout identity, it turns out that it is sufficient to solve it in the case when $q$ is a power $p^n$ of a prime $p$, to get answers for a general $q$.
When $\mathcal{A}(k) = \mathbb{G}_m$ a solution is classical. The answer is affirmative when $q$ is an odd prime and when $q|4$. On the other hand, there are counterexamples for $q = 2^t$, with $t \geq 3$. The most famous of them was discovered by Trost and it is the diophantine equation $x^8 = 16$, that has a solution in $\mathbb{Q}_p$, for all primes $p \in \mathbb{Q}$, $p \neq 2$, but has no solutions in $\mathbb{Q}_2$ and in $\mathbb{Q}$. This is in accordance with the more general Grunwald-Wang theorem.

When $\mathcal{A}(k) \neq \mathbb{G}_m$, a classical way to proceed is to give a cohomological interpretation to the problem. It turns out that the answer is strictly connected to the

behavior of two cohomological groups. The first of them is the cohomological group $H^1(\mathrm{Gal}(\mathbb{Q}(\mathcal{A}[p]/\mathbb{Q}), \mathcal{A}[p])$, where $\mathcal{A}[p]$ is the $p$-torsion subgroup of $\mathcal{A}$. The second is one of its subgroup, named $H^1_{loc}(\mathrm{Gal}(\mathbb{Q}(\mathcal{A}[p])/\mathbb{Q}$, that interprets the hypotheses of the problem in the cohomological context. This last group was defined by R. Dvornicich and U. Zannier in 2001.

They investigated particularly the case when $\mathcal{A}$ is an elliptic curve $\mathcal{E}$. Let $p$ be a prime. The answer to the problem is affirmative when $q = p$ and when $q = p^n$, with $n \geq 2$ and $p \notin S = \{2, 3, 5, 7, 11, 13, 17, 19, 37, 43, 67, 163\}$. This last result was proved in 2007 by R. Dvornicich and U. Zannier. In their proof they used a result found by Mazur to count out the primes in $S$. But in this way, they did not prove an affirmative answer does not hold in those cases too. So an interesting open question that arises from their work, is if does there exist a counterexample for $q = p^n$, with $p \in S$ and $n > 1$. In 2004 they found a counterexample for $q = 2^2$ and an elliptic curve $\mathcal{E}(\mathbb{Q})$ with a Galois group $G := \mathrm{Gal}(\mathbb{Q}(\mathcal{E}[4])/\mathbb{Q})$ isomorphic to $(\mathbb{Z}/2\mathbb{Z})^2$, then in particular of order 4. There were no other known counterexamples so far.

In this thesis we will firstly complete the case when $q = 2^2$ for elliptic curves defined over $\mathbb{Q}$, giving answer for all possible Galois groups $\mathrm{Gal}(\mathbb{Q}(\mathcal{E}[4])/\mathbb{Q})$. In particular, we produce a counterexample for an elliptic curve with $\mathrm{Gal}(\mathbb{Q}(\mathcal{E}[4])/\mathbb{Q}) \cong (\mathbb{Z}/2\mathbb{Z})^3$. Therefore the case of elliptic curves is in analogy with Grunwald-Wang theorem too.

In Chapter 4 of this thesis we will produce more complicated counterexamples for the case when $q = 3^2$. Let $G_3$ be the 3-Sylow subgroup of $\mathrm{Gal}(\mathbb{Q}(\mathcal{E}[9])/\mathbb{Q})$. We will present a family of elliptic curves such that each of them has a group $G_3$ isomorphic to $(\mathbb{Z}/3\mathbb{Z})^2$ and a point locally divisible by 9, but not globally. Furthermore, in Chapter 4, we will produce even another example of an elliptic curve with these characteristics: a group $G_3$ isomorphic to $(\mathbb{Z}/3\mathbb{Z})^3$, a point locally divisible by 9, but not globally.

Since to find counterexamples in the case when $q = 3^2$ was more difficult than in the case when $q = 2^2$, we have assumed to have a $p$-torsion subgroup $\mathcal{E}[3]$ of $\mathcal{E}$ as easy as possible. As a consequence of the Weil Pairing, we have $\mathbb{Q}(\zeta_p) \subseteq \mathbb{Q}(\mathcal{E}[p])$, for all primes $p$. In 2001 L. Merel showed that if $\mathbb{Q}(\mathcal{E}[p]) = \mathbb{Q}(\zeta_p)$, then $p \in \{2, 3, 5, 13\}$ or $p > 1000$. The case $p = 13$ has recently been ruled out by M. Rebolledo. On the contrary, it is known there exist elliptic curves with $\mathbb{Q}(\mathcal{E}[p]) = \mathbb{Q}(\zeta_p)$, when $p \in \{2, 3, 5\}$. We will present the family of all elliptic curves with $\mathbb{Q}(\mathcal{E}[3]) = \mathbb{Q}(\zeta_3)$. In Chapter 3 we will prove that an elliptic curve has the required property if and only if it belongs to that family. Furthermore we will show $\mathbb{Q}(\zeta_5) \subsetneq \mathbb{Q}(\mathcal{E}[5])$ for all elliptic curves with Weierstrass form $y^2 = x^3 + c$ or $y^2 = x^3 + bx$, where $b, c \in \mathbb{Q}$.

# Acknowledgments

I would like to thank Prof. R. Dvornicich for his kindness, his precious suggestions and for having assigned to me a mathematical work I have found interesting to study.
I am grateful to Prof. P. Gianni, for having advised me to use the software Axiom and for her help with that application.
I am also grateful to my colleagues in Pisa, especially Lorenzo Brasco, Marco Illengo and Giulio Peruginelli, and to the other members of the Department of Mathematics in Pisa who have given me their bracer during these years.
Finally, I would like to thank my family, that has always "proved" its love and support to me, and all my other friends in Pisa. You are the best persons I could desire to meet and I am very lucky even because you are too many to be mentioned here.

# Contents

# Chapter 1

# The Local-Global Divisibility Problem

In many cases problems concerning number fields can be solved more easily in their completions. By knowing the local solutions, it is often possible to deduce the global ones. Then, in a natural way, many mathematical problems formulated in last century, have in their hypotheses the existence of local solutions everywhere or almost everywhere. A problem of that type is called a *Local-Global Problem*. Some of them were solved successfully. The most famous one was formulated by Hasse (see [Cas]):

HASSE PRINCIPLE *Let $F(X_1, ..., X_n) \in k[X_1, ..., X_n]$ be a quadratic form, where $k$ is a number field. Suppose the equation $F = 0$ has a nontrivial solution everywhere locally. Then it has a nontrivial solution in $k$.*

It was proved in 1923-24. Other Local-Global Problems remain open in many cases. In this thesis we shall be concerned mainly with the following question:

PROBLEM *Let $k$ be a number field and let $\mathcal{A}$ be a commutative algebraic group defined over $k$. Let $P \in \mathcal{A}(k)$. Denote by $M_k$ the set of the places $v \in k$ and by $k_v$ the completion of $k$ at the valuation $v$. Assume that for all but finitely many $v \in M_k$, there exist $D_v \in \mathcal{A}(k_v)$ such that $P = qD_v$, where $q$ is a positive integer. Is it possible to conclude that there exists $D \in \mathcal{A}(k)$ such that $P = qD$?*

This problem is known as *Local-Global Divisibility Problem*.

## 1.1 Historical solutions for $\mathbb{G}_m$ and a cohomological interpretation of the problem

By using the Bézout identity, it turns out that it is sufficient to solve the Local-Global Divisibility Problem when $q$ is a power of a prime $p$. So, we will suppose $q = p^n$, with $n \in \mathbb{N}$, from now on.

The Local-Global Divisibility Problem has some historical solutions in many cases. When $\mathcal{A}(k)$ is the multiplicative group $\mathbb{G}_m$, there is the following solution for several $q$, due to Artin and Tate (see [AT], Chap IX, Thm. I)

**Theorem 1.1.1.** (Artin, Tate) *Let $k$ be a number field and $M_k$ be the set of the places $v \in k$. Let $q$ be an odd prime or $q = 2^t$, with $t \leq 2$. If $P \in k$ and $P = qD_v$, with $D_v \in k_v$, for all but finitely many $v \in M_k$, then $P = qD$ for any $D \in k$.* □

On the contrary, when $q = 2^n$, with $n \geq 3$, there are some counterexamples showing that the answer to the problem is negative. The most famous of them was discovered by Trost. It is the diophantine equation $x^8 = 16$, that has a solution in $\mathbb{Q}_p$, for all primes $p \in \mathbb{Q}$, $p \neq 2$, but has no solutions in $\mathbb{Q}_2$ and in $\mathbb{Q}$ (see [Tro]). This is in accordance with the more general Grunwald-Wang theorem.

A classical way to proceed for a general $\mathcal{A}(k)$ is to give a cohomological interpretation to the Local-Global Divisibility Problem (see also [DZ]). Let $\overline{k} = \overline{\mathbb{Q}}$ be the algebraic closure of $k$ and let $G_k := \mathrm{Gal}(\overline{k}/k)$ be the absolute Galois group. We denote by $\mathcal{A}[m] \subseteq \mathcal{A}(\overline{k})$ the kernel of the multiplication by $m$. From the classification of the commutative algebraic groups in characteristic zero (see [Ser], Prop 11, 12 §2.7, Chap. III, and §2.7, Chap VIII), we have $\mathcal{A}[m] \cong (\mathbb{Z}/m\mathbb{Z})^n$ for a certain integer $n = n_{\mathcal{A}}$, depending only on $\mathcal{A}$. In particular, for an elliptic curve $\mathcal{E}$, it is well known $\mathcal{E}[m] \cong (\mathbb{Z}/m\mathbb{Z})^2$. If $m = q$, the group $\mathcal{A}[m]$ is clearly an abelian $p$-group. Therefore $G_k$ acts as a subgroup of $\mathrm{GL}_n(\mathbb{Z}/q\mathbb{Z})$ and its image $G$ is isomorphic to $\mathrm{Gal}(k(\mathcal{A}[q])/k)$. Now let $D \in \mathcal{A}(\overline{k})$ such that $P = qD$. We denote by $K$ the field $k(\mathcal{A}[q])$, by $E$ the field $k(D)$, by $F$ the composite field $EK$ and by $\Sigma$ the group $\mathrm{Gal}(F/k)$. For all $\sigma \in \Sigma$, the point $D^\sigma := \sigma(D)$ is again a $q$-divisor of $P$ and then

$$D^\sigma = D + Z_\sigma, \tag{1.1.1}$$

for some $Z_\sigma \in \mathcal{A}[q]$. With a quick computation it is easy to verify

$$Z_{\sigma\tau} = Z_\sigma + \sigma(Z_\tau).$$

Therefore $c : \sigma \mapsto Z_\sigma = D^\sigma - D$ is a cocycle and we denote by $[c]$ its image in $H^1(\Sigma, \mathcal{A}[q])$. The following statement holds (see also [San], Lemma 1.1 (ii))

**Proposition 1.1.2.** *There exists a point $D' \in \mathcal{A}(k)$ such that $P = qD'$ if and only if $[c] = 0$.*

**Proof.** If $[c] = 0$, then there exists a point $W \in \mathcal{A}[q]$ such that $Z_\sigma = W^\sigma - W$, for all $\sigma \in \Sigma$. In this case $D^\sigma - D = W^\sigma - W$ and therefore $(D - W)^\sigma = D - W$ holds for all $\sigma \in \Sigma$. The last equation means $D - W \in \mathcal{A}(k)$. Let $D' := D - W$. Therefore $P = 9D = 9D - 9W = 9D'$, with $D' \in \mathcal{A}(k)$. On the other hand, if $P = qD'$, with $D' \in \mathcal{A}(k)$, then we have $D' = D + W$, with $W \in \mathcal{A}[q]$, because two $q$-divisors of $P$

differs by a $q$-torsion point. Since $D' \in \mathcal{A}(k)$, then $\sigma(D+W) = D+W$, for all $\sigma \in \Sigma$. We have $Z_\sigma = \sigma(D) - D = \sigma(W) - W$. Therefore $[c]$ vanishes in $H^1(\Sigma, \mathcal{A}[q])$. □

Thus $[c] = 0$ if and only if the Local-Global Divisibility Problem has an affirmative answer. This is the reason because it is useful to give a cohomological interpretation to the problem. What do the hypotheses of the problem mean in this context? Let $v$ be a prime of $k$, unramified in $F$ and satisfying the assumptions of the problem. Let $w$ be a prime of $F$ extending $v$. Since $v$ is unramified, the group $\mathrm{Gal}(F_w/k_v)$ is the decomposition group $D(w|v)$. Then $\mathrm{Gal}(F_w/k_v)$ is cyclic, generated by the Frobenius automorphism $[F/k, w]$ of $v$ at $w$. The local divisibility implies $P = qD_v$, for some $D_v \in \mathcal{A}(k_v)$. Therefore $[c]$ vanishes in $H^1(\mathrm{Gal}(F_w/k_v), \mathcal{A}[q])$. By the Tchebotarev density theorem the set of primes $v$ of $k$, which are unramified in $F$ and satisfy the property $[F/k, w] \in Cl$, for any conjugacy class $Cl$ of $\mathrm{Gal}(F/k)$, has positive analytic density $|Cl|/|G|$. Then $\mathrm{Gal}(F_w/k_v) = D(w|v)$ varies over all cyclic subgroups of $\Sigma$ as $w$ runs over almost all primes of $F$. Therefore the local divisibility implies $[c] = 0$ in $H^1(C, \mathcal{A}[q])$, for all cyclic subgroups $C \leq \mathrm{Gal}(F/k)$. In other words, for each $\sigma \in \Sigma$, there exists $W_\sigma \in \mathcal{A}[q]$ such that

$$Z_\sigma = (\sigma - 1)W_\sigma.$$

In a natural way, the following definition arises from the argument above

**Definition** Let $\Gamma$ be a group and let $M$ be a $\Gamma$-module. We say that a cocycle $[c] = [\{Z_\sigma\}] \in H^1(\Gamma, M)$ satisfies the *local conditions* if there exists $W_\sigma \in M$ such that $Z_\sigma = (\sigma - 1)W_\sigma$, for all $\sigma \in \Gamma$. We name the subgroup of $H^1(\Gamma, M)$ formed by such cocycles as the *first local cohomological group* and we denote it by $H^1_{loc}(\Gamma, M)$.

We observe that clearly $H^1_{loc}(\Gamma, M)$ is the intersection of the kernels of the restriction maps $H^1(\Gamma, M) \to H^1(C, M)$, where $C$ varies over all cyclic subgroups of $\Gamma$. If we work with all valuations instead of almost all ones, we get the definition of the group called the *Shafarevich group*. The vanishing of the first local cohomological group gives a sufficient condition to have an affirmative answer to the Local-Global Divisibility Problem. In fact the following result holds

**Theorem 1.1.3.** (Dvornicich, Zannier) *Assume that $H^1_{loc}(G, \mathcal{A}[q]) = 0$. Let $P \in \mathcal{A}(k)$ be a rational point satisfying the assumptions of the Local-Global Divisibility Problem. Then the problem has an affirmative answer.*

**Proof.** Let $P$ satisfy the hypotheses of the Local-Global Divisibility Problem. Let $c := \{Z_\sigma\}_{\sigma \in G}$ be the cocycle defined by (1.1.1), where $D \in \mathcal{A}(\overline{k})$, such that $P = qD$. Then $[c]$ vanishes in $H^1_{loc}(G, \mathcal{A}[q]) = 0$. Since $H^1_{loc}(G, \mathcal{A}[q]) \leq H^1(G, \mathcal{A}[q])$, we have that $[c]$ vanishes in $H^1(G, \mathcal{A}[q])$ too. By proposition 1.1.2, we have that $P$ is divisible by $q$ over $k$. □

Another important observation, useful to answer the problem in many cases, is about the $p$-Sylow subgroup $G_p$ of the group $G$. In fact the following statement holds

**Proposition 1.1.4.** (Dvornicich, Zannier) *An element of $H^1_{loc}(G, \mathcal{A}[q])$ is zero if and only if its restriction to $H^1_{loc}(G_p, \mathcal{A}[q])$ is zero.*

**Proof.** We know $\mathcal{A}[q] \cong (\mathbb{Z}/q\mathbb{Z})^n$ for some $n$. The restriction

$$H^1_{loc}(G, (\mathbb{Z}/q\mathbb{Z})^n) \longrightarrow H^1_{loc}(G_p, (\mathbb{Z}/q\mathbb{Z})^n)$$

is injective on the $p$-primary part of $H^1_{loc}(G, (\mathbb{Z}/q\mathbb{Z})^n)$ (see [Lan], Thm. 4, Chap. IX, §2), which is the whole group in this case, since $(\mathbb{Z}/q\mathbb{Z})^n$ is a $p$-group. On the other hand, a cocycle that satisfies the local conditions for a group $G$, clearly satisfies the local conditions for every subgroup of $G$. □

The last proposition is important because let us work with $G_p$ instead of $G$. We will proceed in this way to found counterexamples. In order to find some of them we will fix our attention about a converse of the theorem 1.1.3, that R. Dvornicich and U. Zannier proved in 2007:

**Theorem 1.1.5.** (Dvornicich, Zannier) *Let $Z$ a be cocycle of $G$ with values in $\mathcal{A}[q]$ representing a nontrivial element of $H^1_{loc}(G, \mathcal{A}[q])$. Then there exists a number field $L$ such that $L \cap K = k$ and a point $P \in \mathcal{A}(L)$ which is divisible by $q$ in $\mathcal{A}(L_w)$ for all unramified places $w$ of $L$, but not divisible by $q$ in $\mathcal{A}(L)$.*

It is possible to find a suitable field $L$ by using the following proposition

**Proposition 1.1.6.** ([DZ3], Prop. 1) *Let $Z$ be a cocycle of $G$ with values in $\mathcal{A}[q]$, whose image in $H^1_{loc}(G, \mathcal{A}[q])$ is nonzero. Then there exists an algebraic variety $\mathcal{B} = \mathcal{B}_Z$ over $k$, isomorphic to $\mathcal{A}$ over $K$, such that, if $L$ is a number field linearly disjoint from $K$ over $k$, $Z$ vanishes in $H^1(G, \mathcal{A}(LK))$ if and only if $\mathcal{B}$ has an $L$-rational point.* □

In the statement of the proposition the group $G$ is identified with $\mathrm{Gal}(LK/L)$. The idea of the proof is to find the algebraic variety $\mathcal{B}$ as a subvariety of the restriction of scalars $\mathcal{H} := R^K_k(\mathcal{A})$ of $\mathcal{A}$ from $K$ to $k$. It is well known that $\mathcal{H}$ is isomorphic over $K$ to the product $\mathcal{H}_K := \prod_{\sigma \in G} \mathcal{A}^\sigma$, (see [Ser2]), where $\mathcal{A}^\sigma$ is now simply $\mathcal{A}$, but viewed over $K$. The subvariety $\mathcal{B}$ is formed by the points $D$ satisfying 1.1.1. Then $\mathcal{B}$ depends on $Z$ and it is possible to verify that has the desired properties (see [DZ3]). Every $L$-rational point over $\mathcal{B}$ leads to a point $P \in \mathcal{A}(L)$ that is locally divisible by $q$ for all places of $L$, unramified in $LK$, but not divisible by $q$ over $L$.

**Proof of Theorem 1.1.5**. Suppose there exists a point $D \in \mathcal{E}_k(L)$, with $L$ linearly disjoint from $k$, and such that $D^\sigma - D = Z_\sigma$, for $\sigma \in G$. Let $P = qD$. By hypothesis, $Z_\sigma \in H^1_{loc}(G, \mathcal{E}[q])$. Then, by the definition of $H^1_{loc}(G, \mathcal{E}[q])$, its restriction to $H^1(C, \mathcal{E}[q])$ is zero, for all cyclic subgroups $C$ of $G$. We identify $G$ with $\mathrm{Gal}((LK)/L)$. Let $w$ be

a place of $L$, unramified in $LK$. We consider an extension of $w$ in $LK$ and we denote it with the same letter. Then the local Galois group $G_w := \mathrm{Gal}((LK)_w/L_w)$ is a cyclic subgroup of $G$. Therefore there exists $T_w \in \mathcal{E}[q]$ that satisfies $T_w^\sigma - T_w = Z_\sigma$, for all $\sigma \in G_w$. The point $D_w := D - T_w$ is fixed by $G_w$. In fact, for all $\sigma \in G_w$, we have

$$D_w^\sigma := D^\sigma - T_w^\sigma = Z_\sigma + D - Z_\sigma - T_w = D - T_w = D_w.$$

Thus $D_w \in L_w$ and $P = qD = q(D - T_w) = qD_w$, because of $T_w \in \mathcal{E}_k[q]$. So the point $P$ is locally divisible by $q$ almost everywhere. Now we show that $P$ is not globally divisible by $q$. Suppose $P = qD_*$, for any $D_* \in L$. Since $D$ and $D_*$ are two of the $q$-divisors of $P$, they differ by a $q$-torsion point of $\mathcal{E}$, i. e. $D = D_* + S$, for some $S \in \mathcal{E}[q]$. Let $\sigma \in G$, then

$$Z_\sigma = D^\sigma - D = (D_* + S)^\sigma - D_* - S = D_*^\sigma - D_* + S^\sigma - S.$$

The point $D_*$ lies in $\mathcal{E}(L)$ by hypothesis, then it is fixed by $G$. We get $Z_\sigma = S^\sigma - S$, for all $\sigma \in G$, that contradicts the hypothesis that $Z_\sigma$ represents a nonzero element in $H^1_{loc}(G, \mathcal{E}[q])$. Therefore $P$ is not globally divisible by $q$. □

## 1.2 Known solutions for elliptic curves

Let $\mathcal{A}$ be an elliptic curve $\mathcal{E}$. If $q = p$, where is a prime, then the problem has an affirmative answer (see also [Won])

**Theorem 1.2.1.** ( [DZ], Thm. 3.1) *Let $\mathcal{E}$ be an elliptic curve defined over a number field $k$. If a point $P \in \mathcal{E}(k)$ is divisible by $p$ in almost all $\mathcal{E}(k_v)$, then it is divisible by $p$ in $\mathcal{E}(k)$.* □

In 2007 R. Dvornicich and U. Zannier gave an affirmative answer for many other $q$, in the case when $\mathcal{A}$ is an elliptic curve. In fact, they proved the following statement (see [DZ3])

**Theorem 1.2.2.** (Dvornicich, Zannier) *Let $\mathcal{E}$ be an elliptic curve defined over a number field $k$ and suppose it does not admit any $k$-rational $p$-isogeny, where $p$ is a prime of $k$. Let $n$ be a nonzero positive integer and let $P \in \mathcal{E}(k)$ be a point divisible by $p^n$ over almost all completions $k_v$. Then $P$ is divisible by $p^n$ over $k$.* □

When $k = \mathbb{Q}$, the previous theorem can be reformulated as follows

**Theorem 1.2.3.** ([DZ3], Thm. 1) *Let $\mathcal{E}$ an elliptic curve defined over $\mathbb{Q}$. Let $P \in \mathcal{E}(\mathbb{Q})$ a point divisible by $p^n$ almost everywhere, where $p$ is a prime number and $n$ a nonzero positive integer. If*

$$p \notin S = \{2, 3, 5, 7, 11, 13, 17, 19, 37, 43, 67, 163\},$$

*then $P$ is divisible by $p^n$ in $\mathcal{E}(\mathbb{Q})$.* □

In the proof of Theorem 1.2.3 R. Dvornicich and U. Zannier used a result found by Mazur (see [Maz]) to count out the primes in $S$. But in this way, they did not prove that an affirmative answer does not hold in those cases too. So, an interesting open question that arises from their work, is if does there exist a counterexample for $q = p^n$, with $p \in S$ and $n > 1$. In 2004 they found a counterexample for $q = 2^2$. They produced an elliptic curve $\mathcal{E}(\mathbb{Q})$ with a Galois group $\mathrm{Gal}(\mathbb{Q}(\mathcal{E}[4])/\mathbb{Q})$ isomorphic to $(\mathbb{Z}/2\mathbb{Z})^2$, then in particular of order 4, and a point $P \in \mathcal{E}(\mathbb{Q})$ locally divisible by 4 almost everywhere over the $p$-adic numbers, but not divisible by 4 over $\mathbb{Q}$ (see [DZ2]).

As in the classical case of $\mathbb{G}_m$ illustrated above, there is an analogy between that and the Grunwald-Wang theorem. In fact in 1933 W. Grunwald proved a result about extensions of number fields $L/k$ with a Galois group $G$ of exponent $n$ (see [Gru] and [Wha]), but in 1948 Sh. Wang found counterexamples to his thesis when $8|n$ (see [Wan]) and in 1950 corrected the error in Grunwald proof (see [Wan2]). He showed that the failing of Grunwald's theorem depend on the behavior of the field of 2-power roots of unity over $k$. Since then the theorem has been called Grunwald-Wang theorem. For completeness we now recall this result. Wang showed the theorem holds for every number field satisfying the following condition

**Wang Condition** *Let $(k, M_k)$ be a multi-valued number field and let $n$ be an integer. Let $2^\nu$ denote the highest power of 2 dividing $n$. We say that $k$ satisfies the Wang condition with respect to $n$ if the field of $2^\nu$-th roots of unity is cyclic over $k$.*

And here is the statement of Grunwald-Wang theorem

**Theorem 1.2.4.** (General Grunwald-Wang theorem)
**(i)** *Let $(k, M_k)$ a multi-valued field with completion $\hat{k}$. Let $G$ be a finite abelian group of exponent $n$ and let a Galois $G$-Algebra $A$ over $\hat{k}$ be given. Then there exists a Galois-$G$-algebra $L/k$ such that its completion $\hat{L}$ satisfies the Wang condition with respect to $n$.*
**(ii)** *It suffices already that every completion $\hat{k}_v$, for $v \in M_v$, satisfies the Wang condition with respect to $n$.*

There are known results concerning the Local-Global Divisibility Problem even when $\mathcal{A}(k)$ is a torus. In this case the answer is affirmative if $p = q$ and $\mathcal{A}(k)$ has dimension $d \leq 3(p-1)$ (see [Ill]). It can be negative for general tori, no matter the prime $p$. A counterexample is shown in [DZ], \$ 5.

# Chapter 2

# Local-global divisibility by $4$ in elliptic curves defined over $\mathbb{Q}$

The only known counterexample to local-global divisibility by 4, for elliptic curves, is the cited Dvornicich-Zannier example. Now we will complete the case when $q = 2^2$ for elliptic curves with Weierstrass form

$$y^2 = (x - \alpha)(x - \beta)(x - \gamma),$$

where $\alpha, \beta, \gamma \in \mathbb{Q}$, are pairwise distinct and satisfy $\alpha+\beta+\gamma = 0$. We give an answer for all possible Galois groups $\mathrm{Gal}(\mathbb{Q}(\mathcal{E}[4])/\mathbb{Q})$. In particular, we produce a counterexample for an elliptic curve with $\mathrm{Gal}(\mathbb{Q}(\mathcal{E}[4])/\mathbb{Q}) \cong (\mathbb{Z}/2\mathbb{Z})^3$.

## 2.1 The completion of the case when $q = 2^2$ for elliptic curves

We prove the following statement

**Theorem 2.1.1.** Let $\mathcal{E}$ be an elliptic curve with Weierstrass form

$$y^2 = (x - \alpha)(x - \beta)(x - \gamma),$$

where $\alpha, \beta$ and $\gamma$ are rational numbers pairwise distinct and satisfy $\alpha + \beta + \gamma = 0$. Let $G$ be the Galois group $\mathrm{Gal}(\mathbb{Q}(\mathcal{E}[4])/\mathbb{Q})$. Then $G \cong (\mathbb{Z}/2\mathbb{Z})^n$, with $n \in \{1, 2, 3, 4\}$, and we have:

*i)* for every elliptic curve $\mathcal{E}$ such that $G \cong (\mathbb{Z}/2\mathbb{Z})^n$, with $n \in \{1, 4\}$, the Local-Global Divisibility Problem when $q = 2^2$ has an affirmative answer for all $P \in \mathcal{E}(\mathbb{Q})$,

*ii)* for every $n \in \{2, 3\}$ there exist elliptic curves $\mathcal{E}$ with $G \cong (\mathbb{Z}/2\mathbb{Z})^n$, and points $P \in \mathcal{E}(\mathbb{Q})$ such that $P \in 4\mathcal{E}(\mathbb{Q}_v)$ for almost all $v \in M_{\mathbb{Q}}$, but $P \notin 4\mathcal{E}(\mathbb{Q})$.

**Proof.** Let $\mathcal{E}$ be an elliptic curve as in the statement of the theorem. We have $\mathbb{Q}(\mathcal{E}[4]) = \mathbb{Q}(\sqrt{-1}, \sqrt{\alpha-\beta}, \sqrt{\beta-\gamma}, \sqrt{\alpha-\gamma})$ (see [DZ2]). Therefore $G \cong (\mathbb{Z}/2\mathbb{Z})^n$, with $n = 1, 2, 3, 4$.

*i*) Since $H^1_{loc}(G, \mathcal{E}[4]) = 0$ when $G$ is cyclic, the Local-Global Divisibility Problem has an affirmative answer for $n = 1$ (see [DZ], Prop 2.1). Let $n = 4$. In this case we have $G \cong (\mathbb{Z}/2\mathbb{Z})^4$. Since $\mathcal{E}[4] \cong (\mathbb{Z}/4\mathbb{Z})^2$, we may identify G with a subgroup of $\mathrm{GL}_2(\mathbb{Z}/4\mathbb{Z})$. We have supposed that the parameters $\alpha, \beta$ and $\gamma$ are rational numbers, then the points of order two of $\mathcal{E}$ are fixed by all automorphisms of $G$. Therefore, every automorphism of $G$ has to be the identity modulo 2. Let $G_0$ be the kernel of the restriction map

$$\mathrm{GL}_2(\mathbb{Z}/4\mathbb{Z}) \longrightarrow \mathrm{GL}_2(\mathbb{Z}/2\mathbb{Z}),$$

and let $H := G \cap G_0$. Clearly we have $H = G$. Then the dimension of $H$ as $\mathbb{F}_2$-vector space is 4. By Proposition 3.2 (iii) of [DZ3], the local-global divisibility by 4 holds for all points $P \in \mathcal{E}$.

*ii*) Now, we suppose $n \in \{2, 3\}$. Because of the cited Dvornicich-Zannier example, we have to find a counterexample only when $n = 3$.

**A counterexample when $|G| = 8$**

Let $G \cong (\mathbb{Z}/2\mathbb{Z})^3$, in particular we have $|G| = 8$. Since $\mathcal{E}[4] \cong (\mathbb{Z}/4\mathbb{Z})^2$, we identify $G$ with a subgroup of $\mathrm{GL}_2(\mathbb{Z}/4\mathbb{Z})$. Consider the group

$$G =< \sigma_1, \sigma_2, \sigma_3 >, \qquad \text{with} \quad \sigma_1 = \begin{pmatrix} -1 & 0 \\ 2 & -1 \end{pmatrix}, \sigma_2 = \begin{pmatrix} 1 & 2 \\ 2 & -1 \end{pmatrix},$$

$$\sigma_3 = \begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix}.$$

$$\text{Let} \qquad \sigma(x, y, z) := \mathrm{I} + 2 \begin{pmatrix} x & y \\ x+y+z & x+y \end{pmatrix}, \qquad \text{with} \quad x, y, z \in \mathbb{Z}/4\mathbb{Z}.$$

Then $\sigma_1 = \sigma(1, 0, 0)$, $\sigma_2 = \sigma(0, 1, 0)$, $\sigma_3 = \sigma(0, 0, 1)$ and $G = \{\sigma(x, y, z) | x, y, z \in \mathbb{Z}/4\mathbb{Z}\}$. Clearly $G \cong (\mathbb{Z}/2\mathbb{Z})^3$. Consider the cocycle

$$Z_{\sigma(x,y,z)} = \begin{pmatrix} 2x \\ 0 \end{pmatrix}.$$

With a quick calculation it is possible to verify that $\{Z_\sigma\}_{\sigma\in G}$ represents a nonzero element in $H^1_{loc}(G, \mathcal{E}[4])$. By Theorem 1.1.5, there exists a counterexample to local-global divisibility by 4 over a finite extension of $\mathbb{Q}$. We will produce a counterexample over $\mathbb{Q}$. We want to find a point $D \in \mathcal{A}(\mathbb{Q}(\mathcal{E}[4]))$, but $D \notin \mathcal{A}(\mathbb{Q})$ satisfying $Z_\sigma = D^\sigma - D$, for all $\sigma \in G$. Since

$$Z_{\sigma_2} = Z_{\sigma_3} = \begin{pmatrix} 0 \\ 0 \end{pmatrix},$$

we have $D = D^{\sigma_2}$ and $D = D^{\sigma_3}$. Therefore the coordinates of $D$ lie in the subfield of $\mathbb{Q}(\mathcal{E}[4])$ fixed by $\sigma_2$ and $\sigma_3$. We denote this field by $K_0$. Clearly $[K_0 : \mathbb{Q}] = 2$ and $\mathrm{Gal}(K_0/\mathbb{Q}) \cong G/ < \sigma_2, \sigma_3 > \cong \mathbb{Z}/2\mathbb{Z}$. Let $K_0 = \mathbb{Q}(\sqrt{\delta})$, with $\delta$ a rational number that is not a square in $\mathbb{Q}$, and let $D = (u, v) = (u_0 + u_1\sqrt{\delta}, v_0 + v_1\sqrt{\delta})$. Furthermore, we have

$$Z_{\sigma_1} = \begin{pmatrix} 2 \\ 0 \end{pmatrix}.$$

Since $2Z_{\sigma_1} = 0$, the point $D^{\sigma_1}$ differs from $D$ by a 2-torsion point. Let $A := (\alpha, 0)$, and suppose that $D^{\sigma_1} = D + A$. By a calculation showed in [DZ2], based on the use of the group law of an elliptic curve, from the last equality we may get the curve

$$\delta s^2 = \delta^2 t^4 - 6\alpha\delta t^2 + (\beta - \gamma)^2, \tag{2.1.1}$$

where $2u_1 = s$, $2u_0 + \alpha = t^2\delta$ and $t\sqrt{\delta} = \dfrac{v}{u-\alpha}$. Clearly $t\sqrt{\delta}$ is the slope of the line passing through $D$ and $A$.

Now, we have to require that $\mathrm{Gal}(\mathbb{Q}(\mathcal{E}[4])/\mathbb{Q})$ corresponds to the group $G$ defined above. We use a basis $\{A', B'\}$ of $\mathcal{E}[4]$ to represent $\mathrm{Gal}(\mathbb{Q}(\mathcal{E}[4])/\mathbb{Q})$ as a subgroup of $\mathrm{GL}_2(\mathbb{Z}/4\mathbb{Z})$. We choose $A', B'$ such that $2A' = A$ and $2B' = B$, where $B := (\beta, 0)$. In fact we have to chose $A'$ such that the point $Z_{\sigma_1} = 2A'$ corresponds to $A$. Specifically, for some given determinations of the square roots, it is possible to verify

$$A' = (\alpha + \sqrt{(\alpha-\beta)(\alpha-\gamma)}, (\alpha-\beta)\sqrt{\alpha-\gamma} + (\alpha-\gamma)\sqrt{\alpha-\beta})$$

$$B' = (\beta + \sqrt{(\beta-\alpha)(\beta-\gamma)}, (\beta-\gamma)\sqrt{\beta-\alpha} + (\beta-\alpha)\sqrt{\beta-\gamma})$$

(see [DZ2]).

We require that $\mathrm{Gal}(\mathbb{Q}(\mathcal{E}[4])/\mathbb{Q})$ corresponds to $G$ with respect to the basis $\{A', B'\}$. By calculating the images of $A'$ and $B'$ under the generators $\sigma_1$, $\sigma_2$ and $\sigma_3$ of $G$, we may check that $\mathrm{Gal}(\mathbb{Q}(\mathcal{E}[4])/\mathbb{Q}) \cong G$ if and only if $(\alpha-\beta)(\beta-\gamma)$ is a rational square and the field $\mathbb{Q}(\mathcal{E}[4]) = \mathbb{Q}(\sqrt{-1}, \sqrt{\alpha-\beta}, \sqrt{\beta-\gamma}, \sqrt{\alpha-\gamma})$ has degree 8 over $\mathbb{Q}$. In Appendix A, by calculating the images of $A'$ and $B'$ under $\sigma_1$, $\sigma_2$ and $\sigma_3$, we show

by direct computation how we can find these conditions. Furthermore, in Appendix A, we show that $K_0 = \mathbb{Q}(\sqrt{\alpha-\beta}, \sqrt{\beta-\gamma})$ and it has degree 2 over $\mathbb{Q}$, as desired. Thus we have $\alpha - \beta = (\beta - \gamma)h^2$, with $h \in \mathbb{Q}$, or $\beta - \gamma = (\alpha - \beta)h^2$. If we suppose $\alpha - \beta = (\beta - \gamma)h^2$, with $h \in \mathbb{Q}$, we have $K_0 = \mathbb{Q}(\sqrt{\beta-\gamma})$ and then $\delta = \beta - \gamma$. The curve (2.1.1), in this case becomes the $(s,t)$-plane curve

$$(\beta-\gamma)s^2 = (\beta-\gamma)^2t^4 - 6\alpha(\beta-\gamma)t^2 + (\beta-\gamma)^2.$$

and since we have assumed $\beta \neq \gamma$, we get the following curve

$$s^2 = (\beta-\gamma)t^4 - 6\alpha t^2 + (\beta-\gamma). \tag{2.1.2}$$

By Theorem 1.1.5 and Proposition 1.1.6, every rational point of that curve gives a counterexample to the local-global divisibility by 4 over $\mathbb{Q}$.

If we suppose $\beta - \gamma = (\alpha - \beta)h^2$, with $h \in \mathbb{Q}$, we have $K_0 = \mathbb{Q}(\sqrt{\alpha-\beta})$ and then $\delta = \alpha - \beta$. The curve (2.1.1), in this case becomes the $(s,t)$-plane curve

$$(\alpha-\beta)s^2 = (\alpha-\beta)^2t^4 - 6\alpha(\alpha-\beta)t^2 + (\alpha-\beta)^2h^4.$$

and since we have assumed $\alpha \neq \beta$, we get the following curve

$$s^2 = (\alpha-\beta)t^4 - 6\alpha t^2 + (\alpha-\beta)h^4. \tag{2.1.3}$$

Again, by Theorem 1.1.5 and Proposition 1.1.6, every rational point of that curve gives a counterexample to the local-global divisibility by 4 over $\mathbb{Q}$.

*A numerical example*

Let $\alpha = -93$, $\beta = -31$ and $\gamma = 62$. We observe that $\beta - \gamma = -31$, $\alpha - \beta = -124 = 4(\beta - \gamma)$ and $\alpha - \gamma = -155 = 5(\beta - \gamma)$. Then $(\alpha - \beta)(\beta - \gamma) = 4(\beta - \gamma)^2$ is a rational square and the field $\mathbb{Q}(\mathcal{E}[4]) = \mathbb{Q}(\sqrt{-1}, \sqrt{\alpha-\beta}, \sqrt{\beta-\gamma}, \sqrt{\alpha-\gamma}) = \mathbb{Q}(\sqrt{-1}, \sqrt{31}, \sqrt{5})$ has degree 8 over $\mathbb{Q}$, as required. Furthermore, we have $K_0 = \mathbb{Q}(\sqrt{-31})$ and $\delta = \beta - \gamma = -31$. For this choice of $\alpha, \beta, \gamma$ we get the elliptic curve

$$\mathcal{E}: \quad y^2 = x(x+93)(x-31)(x-62) = x^3 - 6727x + 178746$$

and the $(s,t)$-plane curve (2.1.2) is

$$s^2 = -31t^4 + 558t^2 - 31.$$

The point $(s,t) = (31,4)$ is a rational point of that curve and we find the corresponding points on $\mathcal{E}$

$$D = \left( -\frac{403}{2} - \frac{31}{2}\sqrt{-31}, 1922 - 434\sqrt{-31} \right)$$

and

$$P = 4D = \left( \frac{5006244481}{16646400}, -\frac{341996266999871}{67917312000} \right).$$

By the arguments of the proof of Theorem 1.1.5, the point $P$ is divisible by 4 over $\mathbb{Q}_v$, for all primes $v \in \mathbb{Q}$ unramified in $\mathbb{Q}(\sqrt{-1}, \sqrt{31}, \sqrt{5})$, but it is not divisible by 4 over $\mathbb{Q}$.

The abscissas of the 16 points $D^*$ such that $4D^* = P$ are the roots of the polynomials:

$$f_1 = 289x^4 - 31992x^3 + 3888206x^2 - 198050568x + 7359538849,$$

$$f_2 = 225x^4 - 59644x^3 + 3027150x^2 + 79482388x - 479307399,$$

$$f_3 = 16x^4 + 4991x^3 + 215264x^2 - 56453945x + 1616161750,$$

$$f_4 = x^4 - 4748x^3 + 13454x^2 + 30509828x - 803433479.$$

In Appendix B we show how it is possible to find these roots. We have that four of them lie in $\mathbb{Q}(\sqrt{31})$, four lie in $\mathbb{Q}(\sqrt{-31})$, four lie in $\mathbb{Q}(\sqrt{5})$ and four lie in $\mathbb{Q}(\sqrt{-1}, \sqrt{155})$. Therefore we may check even by direct computation that $P$ is not globally divisible. □

# Chapter 3

# Elliptic curves with $\mathbb{Q}(\mathcal{E}[p]) = \mathbb{Q}(\zeta_p)$

We are interested on finding an elliptic curve $\mathcal{E}$ with a point $P \in \mathcal{E}$ that gives a counterexample to the Local-Global Divisibility Problem when $q = 3^2$. This case is more difficult than the previous one. Then we suppose that our elliptic curve has a 3-torsion group $\mathcal{E}[3]$ as easy as possible. As a consequence of the Weil Pairing, we know $\mathbb{Q}(\mathcal{E}[p]) \subseteq \mathbb{Q}(\zeta_p)$, for all primes $p$ (see [Sil], III, 8.1.1). In 2001 L. Merel showed that if $\mathbb{Q}(\mathcal{E}[p]) = \mathbb{Q}(\zeta_p)$, then $p \in \{2, 3, 5, 13\}$ or $p > 1000$ (see [Mer]). The case $p = 13$ has recently been ruled out by M. Rebolledo (see [Reb]). On the contrary, it is known there exist elliptic curves with $\mathbb{Q}(\mathcal{E}[p]) = \mathbb{Q}(\zeta_p)$, when $p \in \{2, 3, 5\}$ (see [Mer2]). Now we are interested on finding all elliptic curves with $\mathbb{Q}(\mathcal{E}[3]) = \mathbb{Q}(\zeta_3)$.

## 3.1 The complex case

Let $\mathcal{E}$ be an elliptic curve with Weierstrass form

$$\mathcal{E}: \quad y^2 = x^3 + bx + c, \qquad b, c \in \mathbb{Q}$$

Since $\mathcal{E}[3] \cong (\mathbb{Z}/3\mathbb{Z})^2$, we have 8 points of order 3 on $\mathcal{E}$. Let $x_1, x_2, x_3, x_4$ be the abscissas of those points. It is well known (see [ST]) that they are the roots of the polynomial

$$\Psi_3 = 3x^4 + 6bx^2 + 12cx - b^2.$$

Therefore

$$x^4 + 2bx^2 + 4cx - \frac{b^2}{3} = (x - x_1)(x - x_2)(x - x_3)(x - x_4).$$

At first, we suppose that the roots $x_1, x_2, x_3, x_4$ of $\Psi_3$ are all complex numbers, that means $x_1 = \alpha + \sqrt{-3}\beta$, $x_2 = \alpha - \sqrt{-3}\beta$, $x_3 = \gamma + \sqrt{-3}\delta$, $x_4 = \gamma - \sqrt{-3}\delta$, with $\alpha$, $\beta$, $\gamma$, $\delta \in \mathbb{Q}$, and $\beta, \gamma \neq 0$. Then

$$x^4+2bx^2+4cx-\frac{b^2}{3}=(x-\alpha-\sqrt{-3}\beta)(x-\alpha+\sqrt{-3}\beta)(x-\gamma-\sqrt{-3}\delta)(x-\gamma+\sqrt{-3}\delta).$$

The last coefficient on the right-side of the equation is the nonzero positive number $(\alpha^2+3\beta^2)(\gamma^2+3\delta^2)$ that cannot be equal to the negative number $-b^2/3$. Therefore this case is impossible.

## 3.2 The rational case

Suppose $x_1, x_2, x_3, x_4$ are all rational numbers. This case is a little bit more complicated than the previous one, but we will show it is impossible too. As we have already seen, $x_1, x_2, x_3, x_4$ are the roots of the polynomial

$$\Psi_3 = 3x^4+6bx^2+12cx-b^2.$$

Therefore

$$x^4+2bx^2+4cx-\frac{b^2}{3}=(x-x_1)(x-x_2)(x-x_3)(x-x_4).$$

The equation above is equivalent to the system

$$\begin{cases} x_1+x_2+x_3+x_4=0 & (i)\\ (x_1+x_2)(x_3+x_4)+x_1x_2+x_3x_4=2b & (ii)\\ x_1x_2(x_3+x_4)+x_3x_4(x_1+x_2)=-4c & (iii)\\ x_1x_2x_3x_4=-b^2/3 & (iv) \end{cases} \tag{3.2.1}$$

We observe that 3.2.1$(iv)$ can be written as $x_1x_2=-b^2/(3x_3x_4)$ and 3.2.1$(i)$ can be written as $x_1+x_2=-(x_3+x_4)$. Then the second equation in the system yields

$$-(x_3+x_4)^2+x_3x_4-\frac{b^2}{3x_3x_4}=2b$$

We find

$$b = -3x_3x_4 \pm \sqrt{6x_3^2x_4^2 - 3x_3^3x_4 - 3x_3x_4^3} = -3x_3x_4 \pm \sqrt{-3x_3x_4(x_3 - x_4)^2}$$

$$= -3x_3x_4 \pm (x_3 - x_4)\sqrt{-3x_3x_4}.$$

Since we ask $b$ rational, the last equality yields $-3x_3x_4 = h^2$, with $h \in \mathbb{Q}$. By possibly changing $x_3$ and $x_4$, we can suppose $x_3 = -3x_4l^2$, with $l \in \mathbb{Q}$. Therefore $x_1x_2 = b^2/(9x_4^2l^2)$ and

$$b = -3x_3x_4 \pm (x_3 - x_4)\sqrt{-3x_3x_4} = 9x_4^2l^2 \pm 3x_4l(-3x_4l^2 - x_4), \qquad l, x_4 \in \mathbb{Q}.$$

We can put out $\pm$ in the expression above, because we can choose $l$ be a positive or a negative rational number. Then we have

$$b = 9x_4^2l^2 + 9x_4^2l^3 + 3x_4^2l \quad \text{and} \quad b^2 = 9x_4^4l^2(9l^4 + 18l^3 + 15l^2 + 6l + 1).$$

We have $x_1x_2 = b^2/(9x_4^2l^2) = x_4^2(9l^4 + 18l^3 + 15l^2 + 6l + 1)$. The equation 3.2.1($i$) becomes $x_1 + x_2 = -(x_3 + x_4) = -(-3x_4l^2 + x_4) = (3l^2 - 1)x_4$ and so $x_1 = (3l^2 - 1)x_4 - x_2$. Now, we put together the two equations and we obtain $x_1x_2 = (3l^2 - 1)x_4x_2 - x_2^2 = x_4^2(9l^4 + 18l^3 + 15l^2 + 6l + 1)$. Solving by $x_2$, we have

$$x_2 = \frac{1}{2}(3l^2 - 1)x_4 \pm \frac{1}{2}\sqrt{(3l^2 - 1)^2x_4^2 - 4x_4^2(9l^4 + 18l^3 + 15l^2 + 6l + 1)}$$

$$= \ldots = \frac{1}{2}(3l^2 - 1)x_4 \pm \frac{1}{2}x_4\sqrt{-3(3l + 1)^2(l + 1)^2}$$

$$= \frac{1}{2}(3l^2 - 1)x_4 \pm \frac{1}{2}x_4(3l + 1)(l + 1)\sqrt{-3}$$

and $\quad x_1 = (3l^2 - 1)x_4 - x_2 = \frac{1}{2}(3l^2 - 1)x_4 \pm \frac{1}{2}x_4(3l + 1)(l + 1)\sqrt{-3}.$

Since we are supposing $x_i$ rational for all $i \in \{1, 2, 3, 4\}$, we have only three possibilities: $x_4 = 0$, $l = -1$ and $l = -1/3$.

If we suppose $x_4 = 0$, then $x_1 = x_2 = x_3 = 0$ too. By 3.2.1($ii$) and 3.2.1($iii$), we have $b = c = 0$. If we suppose $l = -1$, we get $x_1 = x_4$, $x_2 = x_4$ and $x_3 = -3x_4$. By 3.2.1($ii$)

and 3.2.1(*iii*), it follows $b = -3x_4^2$ and $c = 2x_4^3$. Therefore we have the family of elliptic curves

$$y^2 = x^3 - 3x_4^2x + 2x_4^3, \qquad \text{with } x_4 \in \mathbb{Q}. \tag{3.2.2}$$

Let $\Delta$ be the discriminant of a curve of this family. We have

$$\Delta = -16(4(-3x_4^2)^3 + 27(2x_4^3)^2) = 0.$$

Thus the curves in (3.2.2) have a singularity and, by definition, they are not elliptic curves. Finally let $l = -1/3$. Therefore $x_1 = x_2 = x_3 = -x_4/3$. So $x_1 = x_2 = x_3$ and $x_4 = -3x_3$. By changing $x_3$ with $x_4$ without loss of generality, we have the previous case again. Then we can conclude there are no elliptic curves $\mathcal{E}$ with $\mathbb{Q}(x_1, x_2, x_3, x_4) = \mathbb{Q}$.

## 3.3 Elliptic curves with $\mathbb{Q}(\mathcal{E}[3]) = \mathbb{Q}(\zeta_3)$

We have showed that two roots of $\Psi_3$ are rational numbers and two are complex ones. Suppose $x_3 = \alpha + i\beta$ and $x_4 = \alpha - \sqrt{-3}\beta$, with $\alpha, \beta \in \mathbb{Q}$, $\beta \neq 0$. Then

$$x^4 + 2bx^2 + 4cx - \frac{b^2}{3} = (x - x_1)(x - x_2)(x - \alpha - \sqrt{-3}\beta)(x - \alpha + \sqrt{-3}\beta).$$

By comparing the coefficient in the previous equation, we get the system

$$\begin{cases} x_1 + x_2 = -2\alpha & (i) \\ \alpha^2 + 3\beta^2 + 2\alpha(x_1 + x_2) + x_1x_2 = 2b & (ii) \\ (\alpha^2 + 3\beta^2)(x_1 + x_2) + 2\alpha x_1x_2 = -4c & (iii) \\ (\alpha^2 + 3\beta^2)x_1x_2 = -b^2/3 & (iv) \end{cases} \tag{3.3.1}$$

We observe that the equation 3.3.1(*iv*) can be written as $x_1x_2 = -b^2/(3(\alpha^2+3\beta^2))$. By using the last equality and 3.3.1(*i*), the equation 3.3.1(*ii*) yields

$$\alpha^2 + 3\beta^2 - 4\alpha^2 - \frac{b^2}{3(\alpha^2 + 3\beta^2)} = 2b.$$

We find

$$b = -3(\alpha^2 + 3\beta^2) \pm \sqrt{(36\alpha^2\beta^2 + 108\beta^4)}.$$

Then

$$b = -3(\alpha^2 + 3\beta^2) \pm 6\beta\sqrt{(\alpha^2 + 3\beta^2)}.$$

Since we ask that $b$ is a rational number, we have that $\alpha^2 + 3\beta^2$ has to be a rational square. Therefore let $m^2 = \alpha^2 + 3\beta^2$, $m \in \mathbb{Q}$ . Then

$$b = -3m^2 \pm 6\beta m. \tag{3.3.2}$$

We put out $\pm$ in the last expression of $b$, because we can choose $m = \pm\sqrt{\alpha^2 + 3\beta^2}$ be positive or negative. By using 3.3.1($i$), 3.3.1($iv$) and 3.3.2 in the equation 3.3.1($iii$), we can find the value of $c$ in terms of $\alpha$ and $\beta$

$$c = 2\alpha^3 + 12\alpha\beta^2 - 6\alpha\beta m. \tag{3.3.3}$$

Furthermore, from the system 3.3.1 we can find the values of $x_1$ and $x_2$ in terms of $\alpha$, $\beta$ and $m$ too. We may verify

$$x_{1/2} = -\alpha \pm \sqrt{4\alpha^2 + 21\beta^2 - 12\beta m} =$$

$$= -\alpha \pm \sqrt{(2m - 3\beta)^2} = \ -\alpha \pm (2m - 3\beta).$$

We have the family of elliptic curves

$$\mathcal{F}_{\alpha,\beta}: \quad y^2 = x^3 + (-3m^2 + 6\beta m)x + 2\alpha^3 + 12\alpha\beta^2 - 6\alpha\beta m, \tag{3.3.4}$$

with $\alpha, \beta \in \mathbb{Q}$, $\beta \neq 0$, $m^2 = \alpha^2 + 3\beta^2$ and $m$ a rational square.

Every elliptic curve in that family has the property that the abscissas of its points of order three are in $\mathbb{Q}(\zeta_3)$. But we ask more that the ordinates also of those points are in $\mathbb{Q}(\zeta_3)$. So we have to find another condition for $\alpha$, $\beta$ and $m$ implying that. Let $\pm y_i$ be the ordinates corresponding respectively to $x_i$, for $i \in \{1, 2, 3, 4\}$, and let $P_i = (x_i, y_i)$. Suppose $P_1, P_2 \in \mathcal{E}(\mathbb{Q}(\zeta_3))$. Since $P_1$, $P_2$ form a basis of $\mathcal{E}[3] \cong (\mathbb{Z}/3\mathbb{Z})^2$, we have that $P_3 = P_1 + P_2$ and $P_4 = P_1 - P_2$ are in $\mathcal{E}(\mathbb{Q}(\zeta_3))$ too. So it suffices to ask $y_1, y_2 \in \mathbb{Q}$. The points $P_1, P_2$ lie on an elliptic curve $\mathcal{E}_{\alpha,\beta} \in \mathcal{F}_{\alpha,\beta}$, then

$$y_1^2 = x_1^3 + (-3m^2 + 6\beta m)x_1 + 2\alpha^3 + 12\alpha\beta^2 - 6\alpha\beta m.$$

By using the expression of $x_1$ in terms of $\alpha$ and $\beta$ found above, we have

$$y_1^2 = (-\alpha + 2m - 3\beta)^3 + (-3m^2 + 6\beta m)(-\alpha + 2m - 3\beta) + 2\alpha^3 + 12\alpha\beta^2 - 6\alpha\beta m = ... =$$

$$= \alpha^3 + 2m^3 - 27\beta^3 + 6\alpha^2 m - 9\alpha^2\beta - 9\alpha m^2 - 15\beta m^2 - 15\alpha\beta^2 + 36\beta^2 m + 24\alpha\beta m.$$

By the substitution $m^2 = \alpha^2 + 3\beta^2$, we can check that

$$y_1^2 = -2(\alpha - m)(4\alpha^2 + 21\beta^2 - 12\beta m) = -2(\alpha - m)(2m - 3\beta)^2.$$

Therefore

$$y_1 = \pm(2m - 3\beta)\sqrt{-2(\alpha - m)}.$$

The condition for $y_1 \in \mathbb{Q}(\zeta_3)$ is then $\sqrt{-2(\alpha - m)} \in \mathbb{Q}(\zeta_3)$. It means that $-2(\alpha - m)$ has to be a square in $\mathbb{Q}(\zeta_3)$. Since $\alpha, m \in \mathbb{Q}$, we have that the condition for $y_1 \in \mathbb{Q}(\zeta_3)$ is

$$-2(\alpha - m) = h^2 \quad \text{or} \quad -2(\alpha - m) = -3h^2, \quad \text{with } h \in \mathbb{Q}.$$

It's easy to verify in the same way, that $y_2 = \pm(2m - 3\beta)\sqrt{-2(\alpha + m)}$. The last equality implies that $-2(2\alpha + m)$ also has to be a square in $\mathbb{Q}(\zeta_3)$. Since $\alpha, m \in \mathbb{Q}$, the condition for $y_2 \in \mathbb{Q}(\zeta_3)$ is

$$-2(\alpha + m) = k^2 \quad \text{or} \quad -2(\alpha + m) = -3k^2, \quad \text{with } k \in \mathbb{Q}.$$

We observe that

$$-3(4\beta^2) = 4(-3\beta^2) = 4(\alpha^2 - m^2) = [-2(\alpha - m)][-2(\alpha + m)]. \tag{3.3.5}$$

Then $-2(\alpha - m) = -3h^2$ clearly implies $-2(\alpha + m) = k^2$ and $-2(\alpha - m) = h^2$ implies $-2(\alpha + m) = -3k^2$. So the condition "$-2(\alpha - m)$ is a square in $\mathbb{Q}(\zeta_3)$" together with the condition $m^2 = \alpha^2 + 3\beta^2$, are sufficient to have $\mathbb{Q}(\mathcal{E}_{\alpha,\beta}[3]) = \mathbb{Q}(\zeta_3)$. Furthermore, we have shown that every elliptic curve $\mathcal{E}_{\alpha,\beta}$ with this property has a rational point of order three.

In order to list all elliptic curves with $\mathbb{Q}(\mathcal{E}[3]) = \mathbb{Q}(\zeta_3)$, we now put together the conditions $m^2 = \alpha^2 + 3\beta^2$ and "$-2(\alpha - m)$ is a square in $\mathbb{Q}(\zeta_3)$". At first we suppose $-2(\alpha - m) = h^2$, with $h \in \mathbb{Q}$. Therefore $-2\alpha + 2m = h^2$ and then $m = h^2/2 + \alpha$. We have

$$\alpha^2 + 3\beta^2 = m^2 = \frac{h^4}{4} + \alpha^2 + \alpha h^2.$$

Therefore

$$\alpha = \frac{3\beta^2}{h^2} - \frac{h^2}{4}, \qquad h \neq 0,$$

and

$$m = \frac{h^2}{2} + \alpha = \frac{h^2}{2} + \frac{3\beta^2}{h^2} - \frac{h^2}{4} = \frac{h^2}{4} + \frac{3\beta^2}{h^2}.$$

We observe that if $h = 0$, then $m = \alpha$. Clearly the last equality implies $\beta = 0$, a contradiction with our hypothesis. Now, we suppose $-2(\alpha - m) = -3k^2$, for $k \in \mathbb{Q}$. By the observation above, this implies $-2(\alpha + m) = h^2$, for $h \in \mathbb{Q}$. We find $\alpha = 3\beta^2/h^2 - h^2/4$ again, and $m = -3\beta^2/h^2 - h^2/4$.

The family of elliptic curves with $\mathbb{Q}(\mathcal{E}[3]) = \mathbb{Q}(\zeta_3)$ is

$$\mathcal{F}_{\beta,h}: \quad y^2 = x^3 + (-3m^2 + 6\beta m)x + 2\alpha^3 + 12\alpha\beta^2 - 6\alpha\beta m, \tag{3.3.6}$$

$$\text{with} \quad \alpha = \frac{3\beta^2}{h^2} - \frac{h^2}{4}\ , \qquad m = \frac{h^2}{4} + \frac{3\beta^2}{h^2}\ , \qquad \beta, h \in \mathbb{Q} \setminus \{0\}.$$

In (3.3.6) we consider $m$ only positive, because it is always multiplied by $\beta$, that can be chosen positive or negative. By replacing in (3.3.6) the numbers $\alpha$ and $m$ with their values in terms of $\beta$ and $h$, we prove the following statement

**Theorem 3.3.1.** *Let $\mathcal{E}$ be an elliptic curve with Weierstrass form $y^2 = x^3 + bx + c$, where $b, c \in \mathbb{Q}$. Its 3-torsion subgroup $\mathcal{E}[3]$ is such that $\mathbb{Q}(\mathcal{E}[3]) = \mathbb{Q}(\zeta_3)$ if and only if $\mathcal{E}$ belongs to the family*

$$\mathcal{F}_{\beta,h}: \quad y^2 = x^3 + b_{\beta,h}x + c_{\beta,h}, \qquad \beta, h \in \mathbb{Q} \setminus \{0\}, \tag{3.3.7}$$

$$\begin{aligned} \textit{with} \qquad b_{\beta,h} &= -27\ \frac{\beta^4}{h^4} + 18\ \frac{\beta^3}{h^2} - 9\ \frac{\beta^2}{2} + 3\ \frac{\beta h^2}{2} - 3\ \frac{h^4}{16}, \\ c_{\beta,h} &= 54\ \frac{\beta^6}{h^6} - 54\ \frac{\beta^5}{h^4} + 45\ \frac{\beta^4}{2h^2} - 15\ \frac{\beta^2 h^2}{8} - 3\ \frac{\beta h^4}{8} - \frac{1}{32h^6}. \end{aligned}$$ □

Furthermore, we recall that by the observation (3.3.5), we have proved the following result

**Corollary 3.3.2.** *Let $\mathcal{E}$ be an elliptic curve, with Weierstrass form $y^2 = x^3 + bx + c$, $b, c \in \mathbb{Q}$, and such that $\mathbb{Q}(\mathcal{E}[3]) = \mathbb{Q}(\zeta_3)$. Then $\mathcal{E}$ has a rational point of order 3.* □

We have shown that there are infinitely many elliptic curves $\mathcal{E}$ with $\mathbb{Q}(\mathcal{E}[3]) = \mathbb{Q}(\zeta_3)$. They form a family depending on two nonzero rational parameters. We want to know when two curves in that family are isomorphic. In general, if $\overline{k}$ is the algebraic closure of a number field $k$, two elliptic curves are isomorphic over $\overline{k}$ if and only if they have the same $j$-invariant. Furthermore, if $j = 0$ then $\mathrm{Aut}(\mathcal{E}) \cong \mathbb{Z}/6\mathbb{Z}$, if $j = 1728$ then $\mathrm{Aut}(\mathcal{E}) \cong \mathbb{Z}/4\mathbb{Z}$, if $j \neq 0, 1728$ then $\mathrm{Aut}(\mathcal{E}) \cong \mathbb{Z}/2\mathbb{Z}$. Let $\Delta$ be the discriminant of an elliptic curve with Weierstrass form $y^2 = x^3 + bx + c$, then

$$\Delta = -16(4b^3 + 27c^2), \qquad j = -\frac{1728(4b)^3}{\Delta}.$$

In our case

$$\Delta = -\frac{216\beta^3(h^4 - 6\beta^2h^2 + 12\beta^3)}{h^6},$$

$$j = -\frac{27(h^2 - 6\beta)^3(h^2 - 2\beta)^3(h^4 + 12\beta^2)^3}{8\beta^3h^6(h^4 - 6\beta h^2 + 12\beta^2)^3}.$$

A curve in the family (3.3.7) has a singular point if and only if $\Delta = 0$, if and only if $\beta = 0$. Since we are supposing $\beta \neq 0$, we can conclude there are no curves with singularities in $\mathcal{F}_{\beta,h}$. We are interested in finding all isomorphism classes of the curves of that family. If we fix one of those curves, by choosing $\beta = \overline{\beta}$ and $h = \overline{h}$, and we denote by $\overline{j}$ its $j$-invariant, it is possible to verify that $j - \overline{j}$ is a polynomial in the variables $\beta$ and $h$ with numerator

$$\begin{aligned}
p_j :=& 27 \cdot (\beta\overline{h}^2 - \overline{\beta}h^2) \cdot (h^2\overline{h}^2 - 12b\overline{\beta}) \\
&\cdot (\beta^2\overline{h}^4 + (\beta\overline{\beta}h^2 - 6\beta^2\overline{\beta})\overline{h}^2 + \overline{\beta}^2h^4 - 6\beta\overline{\beta}^2h^2 + 12\beta^2\overline{\beta}^2) \\
&\cdot ((h^4 - 6\beta h^2 + 12\beta^2)\overline{h}^4 + (-6\overline{\beta}h^4 + 12b\overline{\beta}h^2)\overline{h}^2 + 12\overline{\beta}^2h^4) \\
&\cdot ((h^4 - 6\beta h^2 + 12\beta^2)\overline{h}^4 + (12\beta\overline{\beta}h^2 - 72b^2\overline{\beta})\overline{h}^2 + 144b^2\overline{\beta}^2) \\
&\cdot (h^4\overline{h}^4 + (-6\overline{\beta}h^4 + 12\beta\overline{\beta}h^2)\overline{h}^2 + 12\overline{\beta}^2h^4 - 72\beta\overline{\beta}^2h^2 + 144\beta^2\overline{\beta}^2) \\
&\cdot ((h^4 - 6\beta h^2 + 12\beta^2)\overline{h}^4 + (-6\overline{\beta}h^4 + 48\beta\overline{\beta}h^2 - 72\beta^2\overline{\beta})\overline{h}^2 + 12\overline{\beta}^2h^4 \\
&\qquad - 72\beta\overline{\beta}^2h^2 + 144\beta^2\overline{\beta}^2).
\end{aligned}$$

If $p_j = 0$, then $\mathcal{E}_{\beta,h} \cong \mathcal{E}_{\overline{\beta},\overline{h}}$. Clearly, we have $(\beta\overline{h}^2 - \overline{\beta}h^2) = 0$ if and only if $\beta = h^2\overline{\beta}/\overline{h}^2$ and we have $(h^2\overline{h}^2 - 12\beta\overline{\beta}) = 0$ if and only if $\beta = -h^2\overline{h}^2/(12\overline{\beta})$. There are no other possible relations for rational parameters $\beta, \overline{\beta}, h, \overline{h}$ coming from the other factors of $p_j$. In fact if we suppose, for instance,

$$\beta^2\overline{h}^4 + (\beta\overline{\beta}h^2 - 6\beta^2\overline{\beta})\overline{h}^2 + \overline{\beta}^2h^4 - 6\beta\overline{\beta}^2h^2 + 12\beta^2\overline{\beta}^2 = 0, \tag{3.3.8}$$

we get

$$\beta = \frac{-\overline{\beta}h^2\overline{h}^2 + 6\overline{\beta}^2h^2 \pm \sqrt{-3\overline{\beta}^2h^4\overline{h}^4 + 12\overline{\beta}^3h^4\overline{h}^2 - 12\overline{\beta}^4h^4}}{2\overline{h}^4 - 12\overline{\beta}\,\overline{h}^2 + 24\overline{\beta}^2}.$$

Since $\beta$ is a rational number, the argument of the square root has to be a square. But we observe that this is impossible for every choice of the parameters $\overline{beta}, \overline{h}$ and $h$, because of

$$-3\overline{\beta}^2h^4\overline{h}^4 + 12\overline{\beta}^3h^4\overline{h}^2 - 12\overline{\beta}^4h^4 = -3h^4\overline{\beta}^2(\overline{h}^4 + 4\overline{\beta}^2\overline{h}^2 + 4\overline{\beta}^4) = -3h^4\overline{\beta}^2(\overline{h}^2 + 2\overline{\beta}^2)^2.$$

We may show in the same way that there are no possible relations coming from the other factors of $p_j$. Then we have proved the following statement

**Theorem 3.3.3.** *Let $\mathcal{E}_{\overline{\beta},\overline{h}} \in \mathcal{F}_{\beta,h}$. An elliptic curve $\mathcal{E}_{\beta,h}$ of the same family is isomorphic to $\mathcal{E}_{\overline{\beta},\overline{h}}$ if and only if $\beta = h^2\overline{\beta}/\overline{h}^2$ or $\beta = -h^2\overline{h}^2/(12\overline{\beta})$, for any $h \in \mathbb{Q} \setminus \{0\}$.* □

We observe that if we choose $\overline{h}' = 1/\overline{h}$ and $\overline{\beta}' = -1/(12\overline{\beta})$, we have $\beta = -h^2\overline{h}^2/(12\overline{\beta}) = h^2\overline{\beta}'/(\overline{h}')^2$. Then the number of isomorphism classes depends only on $\overline{\beta}/\overline{h}^2$. Since it varies over all nonzero rational numbers, there are infinite isomorphism classes. Furthermore, there are infinite representatives for each of them, because of $h \in \mathbb{Q} \setminus \{0\}$. We are particularly interested in seeing if there is an isomorphism class with $j = 0$ and an isomorphism class with $j = 1728$. It is easy to verify that the case $j = 1728$ is impossible. On the contrary, we can get $j = 0$, by choosing $\beta = h^2/2$ or $\beta = h^2/6$. When $\beta = h^2/2$, we find $b = 0$ and $c = h^6/4 = 16(h/2)^6$. By putting $k := h/2$, we get the subfamily

$$\mathcal{E}_k : y^2 = x^3 + 16k^6, \qquad k \in \mathbb{Q}.$$

When $\beta = h^2/6$, we find $b = 0$ and $c = -h^6/108 = -432(h/6)^6$. By putting $l := h/6$, we find the subfamily

$$\mathcal{E}_l : y^2 = x^3 - 432l^6, \qquad l \in \mathbb{Q}.$$

Therefore the curves of this two families $\mathcal{E}_k$ and $\mathcal{E}_l$ are all isomorphic and, furthermore, they are the only curves in $\mathcal{F}_{\beta,h}$, with $\mathrm{Aut}(\mathcal{E}) \cong \mathbb{Z}/6\mathbb{Z}$. Clearly $\mathrm{Aut}(\mathcal{E}_k) = \mathrm{Aut}(\mathcal{E}_l) =< -\mathrm{I}, \tilde{\tau} >$, where

$$-\mathrm{I}: \quad (x, y) \longmapsto (x, -y),$$

$$\tilde{\tau}: \quad (x, y) \longmapsto (x\zeta_3, y),$$

for all $(x, y) \in \mathcal{E}_k, \mathcal{E}_l$. All other curves in $\mathcal{F}_{\beta,h}$ have an automorphism group isomorphic to $\mathbb{Z}/2\mathbb{Z}$ and generated by -I. We have proved the following corollary

**Corollary 3.3.4.** *Let $\mathcal{E}$ an elliptic curve with Weierstrass form $y^2 = x^3 + bx + c$, $b, c \in \mathbb{Q}$, and such that $\mathbb{Q}(\zeta_3) = \mathbb{Q}(\mathcal{E}[3])$. If $b = 0$, then $\mathrm{Aut}(\mathcal{E}) \cong \mathbb{Z}/6\mathbb{Z}$. If $b \neq 0$, then $\mathrm{Aut}(\mathcal{E}) \cong \mathbb{Z}/2\mathbb{Z}$.* □

## 3.4 Some results about elliptic curves with $\mathbb{Q}(\zeta_5) \subsetneq \mathbb{Q}(\mathcal{E}[5])$

In the previous section we have found all elliptic curves with $\mathbb{Q}(\zeta_3) = \mathbb{Q}(\mathcal{E}[3])$. We know there exist even elliptic curves such that $\mathbb{Q}(\zeta_5) = \mathbb{Q}(\mathcal{E}[5])$ (see [Mer2]), but the family of all of them is not known. We will prove that for all elliptic curve $\mathcal{E}$ with Weierstrass form $y^2 = x^3 + bx + c$, where $b$ and $c$ are rational numbers and $b = 0$ or $c = 0$, we cannot have $\mathbb{Q}(\zeta_5) = \mathbb{Q}(\mathcal{E}[5])$.

**Theorem 3.4.1.** *Let $\mathcal{E}$ be an elliptic curve with Weierstrass form $y^2 = x^3 + bx + c$, $b, c \in \mathbb{Q}$. If $b = 0$ or $c = 0$, then $\mathbb{Q}(\zeta_5) \subsetneq \mathbb{Q}(\mathcal{E}[5])$.*

**Proof.** The abscissas of the points of order 5 of $\mathcal{E}$ are the roots of the polynomial

$$\psi_5 := -5x^{12} - 62bx^{10} - 380cx^9 + 105b^2x^8 - 240bcx^7 + (240c^2 + 300b^3)x^6 + 696b^2cx^5 +$$
$$(1920bc^2 + 125b^4)x^4 + (1600c^3 + 80b^3c)x^3 + (240b^2c^2 + 50b^5)x^2 + (640bc^3 + 100b^4c)x +$$
$$256c^4 + 32b^3c^2 - b^6.$$

If $b = 0$ the abscissas of the points of order 5 of $\mathcal{E}$ are the roots of the polynomial

$$\varphi_1 := -5x^{12} - 380cx^9 + 240c^2x^6 + 1600c^3x^3 + 256c^4.$$

By the use of Axiom or another software of computational algebra, it is possible to verify the factorization of $\varphi_1$ over $\mathbb{Q}(\zeta_5)$ is

$$\varphi_1 = -5 \cdot (x^6 + (-36\zeta_5^3 - 36\zeta_5^2 + 20)cx^3 + \frac{-288\zeta_5^3 - 288\zeta_5^2 + 176}{5}c^2)$$

$$\cdot(x^6 + (36\zeta_5^3 + 36\zeta_5^2 + 56)cx^3 + \frac{288\zeta_5^3 - 288\zeta_5^2 + 464}{5}c^2)$$

and the factorization of $\varphi_1$ over $\mathbb{Q}(\zeta_3, \zeta_5)$ is

$$\varphi_1 = -5 \cdot (x^3 + \frac{(-132\zeta_3 + 24)\zeta_5^3 + (36\zeta_3 + 108)\zeta_5^2 + (-96\zeta_3 - 48)\zeta_5 - 48\zeta_3 + 116}{5}c)$$

$$\cdot(x^3 + \frac{(-36\zeta_3 - 108)\zeta_5^3 + (-132\zeta_3 - 156)\zeta_5^2 + (-168\zeta_3 - 84)\zeta_5 - 84\zeta_3 + 92}{5}c)$$

$$\cdot(x^3 + \frac{(132\zeta_3 + 156)\zeta_5^3 + (-36\zeta_3 + 72)\zeta_5^2 + (96\zeta_3 + 48)\zeta_5 + 48\zeta_3 + 164}{5}c)$$

$$\cdot(x^3 + \frac{(36\zeta_3 - 72)\zeta_5^3 + (132\zeta_3 - 24)\zeta_5^2 + (168\zeta_3 + 84)\zeta_5 + 84\zeta_3 + 92}{5}c)$$

A basis of $\mathbb{Q}(\zeta_3, \zeta_5)/\mathbb{Q}$ is formed by $\zeta_3^i\zeta_5^j$, with $i \in \{0, 1\}$ and $j \in \{0, 1, 2, 3, 4\}$. Therefore these elements are linearly independent and it follows that the constant terms of the factors of $\varphi_1$ are not in $\mathbb{Q}(\zeta_5)$, for all $c \in \mathbb{Q}$. Then $\mathbb{Q}(\zeta_3) \subseteq \mathbb{Q}(\mathcal{E}[5])$, for all $\mathcal{E}$ with $b = 0$.

If $c = 0$ the abscissas of the points of order 5 of $\mathcal{E}$ are the roots of the polynomial

$$\varphi_2 := -5x^{12} - 62bx^{10} + 105b^2x^8 + 300b^3x^6 + 125b^4x^4 + 50b^5x^2 - b^6.$$

By the use of Axiom or another software of computational algebra, it is possible to verify that the factorization of $\varphi_2$ over $\mathbb{Q}(\zeta_5)$ is

$$\varphi_2 = -5 \cdot (x^4 + (-8\zeta_5^3 - 8\zeta_5^2 + 2)bx^2 + (-8\zeta_5^3 - 8\zeta_5^2 + 5)b) \cdot (x^4 + \frac{2}{5}bx^2 + \frac{1}{5}b^2)$$

$$\cdot(x^4 + (8\zeta_5^3 + 8\zeta_5^2 + 10)bx^2 + (8\zeta_5^3 + 8\zeta_5^2 + 13)b)$$

and the factorization of $\varphi_2$ over $\mathbb{Q}(i, \zeta_5)$, where $i = \sqrt{-1}$, is

$$\varphi_2 = -5\cdot(x^2+((-4i+4)\zeta_5^3+4\zeta_5^2-4I\zeta_5-2i+5)b)\cdot(x^2+(-4\zeta_5^3+(-4i-4)\zeta_5^2+4I\zeta_5+2i+1)b)$$

$$\cdot(x^2+((4i+4)\zeta_5^3+4\zeta_5^2+4I\zeta_5+2i+5)b)\cdot(x^2+(-4\zeta_5^3+(4i-4)\zeta_5^2+4I\zeta_5+2i+1)b)$$

$$\cdot(x^2+\frac{-2i+1}{5}b)\cdot(x^2+\frac{2i+1}{5}b)$$

For every rational value of $b$, the terms $(-2i+1)b/5$ and $(2i+1)b/5$ are not in $\mathbb{Q}$, then $\mathbb{Q}(i) \subseteq \mathbb{Q}(\mathcal{E}[5])$, for all $\mathcal{E}$ with $c = 0$. □

# Chapter 4

# Counterexamples to local-global divisibility by 9 for elliptic curves

We will consider the elliptic curves of the subfamily $\mathcal{E}_k$ of $\mathcal{F}_{\alpha,\beta}$, found in 3.3, and we will prove that the Galois group $\mathrm{Gal}(\mathbb{Q}(\mathcal{E}_k[9])/\mathbb{Q})$ does not depend on $k$ and, in particular, has a 3-Sylow subgroup isomorphic to $(\mathbb{Z}/3\mathbb{Z})^2$. Then, we will prove that, for all $k$, there exists a point $P_k \in \mathcal{E}_k$ locally divisible by 9 almost everywhere, but not globally, over a number field of degree at most 2 over $\mathbb{Q}(\zeta_3)$. Finally, we produce another example of an elliptic curve with these properties: a group $\mathrm{Gal}(\mathbb{Q}(\mathcal{E}[9])/\mathbb{Q})$, whose 3-Sylow subgroup is isomorphic to $(\mathbb{Z}/3\mathbb{Z})^3$, and a point locally divisible by 9 almost everywhere, but not globally, over a field of degree 2 over $\mathbb{Q}(\zeta_3)$.

## 4.1 A special subfamily of $\mathcal{F}_{\alpha,\beta}$

We consider the subfamily $\mathcal{E}_k$ of $\mathcal{F}_{\alpha,\beta}$, found in 3.3. We have $\mathcal{E}_k$: $y^2 = x^3 + 16k^6$, with $k \in \mathbb{Q}$. We already know $\mathbb{Q}(\mathcal{E}_k[3]) = \mathbb{Q}(\zeta_3)$. Now, we will show that $[\mathbb{Q}(\mathcal{E}_k[9]) : \mathbb{Q}(\zeta_3)] = 9$, for all $k \in \mathbb{Q}$. In the same way it is possible to verify that $[\mathbb{Q}(\mathcal{E}_l[9]) : \mathbb{Q}(\zeta_3)] = 9$, where $\mathcal{E}_l$: $y^2 = x^3 - 432l^6$, $l \in \mathbb{Q}$. Since the two families have the same characteristics, we chose to work with $\mathcal{E}_k$. Using the results shown in 3.3, we have

$$\mathcal{E}[3] = \{(0, \pm 4k^3), (-4k^2, \pm 4k^3), (k/2 + k/2\sqrt{-3}, \pm 4k^3), (k/2 - k/2\sqrt{-3}, \pm 4k^3)\}.$$

Let $Q = (x, y)$ be a point on $\mathcal{E}_k$, for any $k \in \mathbb{Q}$. We use the group law of an elliptic curve to find the abscissas of the point $3Q$

$$x_{3Q} = \frac{81x^9 - 144y^4x^3 + 64y^6}{81x^8 - 216y^2x^5 + 144y^4x^2}$$

By putting $y^2 = x^3 + 16k^6$ in the expression above, we get

$$x_{3Q} = \frac{x^9 - 1536k^6x^6 + 12288k^{12}x^3 + 262144k^{18}}{9x^8 + 1152k^6x^5 + 36864k^{12}x^2}. \tag{4.1.1}$$

Let $A_1 := (0, 4k^3)$ and $A_2 := (-4k^2, 4k^3)$ be two of the points of order 3 of $\mathcal{E}$. Then the roots of the numerators $\phi_i$ of the polynomials $x_{3Q} - x_{A_i}$, for $i = 1, 2$, are the abscissas of some points of order 9 of $\mathcal{E}$. We can choose two of these roots, one for each of the two polynomials, to find a basis of $\mathcal{E}[9] \cong (\mathbb{Z}/9\mathbb{Z})^2$ and then to know the field extension $\mathbb{Q}(\mathcal{E}[9])$. Thus we look for the roots of

$$\phi_1 : \quad x^9 - 1536k^6x^6 + 12288k^{12}x^3 + 262144k^{18}$$

and

$$\phi_2 : \quad x^9 - 1536k^6x^6 + 12288k^{12}x^3 + 262144k^{18} + 4k^2(9x^8 + 1152k^6x^5 + 36864k^{12}x^2) =$$

$$= x^9 + 36k^2x^8 - 1536k^6x^6 + 4608k^8x^5 + 12288k^{12}x^3 + 147456k^{14}x^2 + 262144k^{18}.$$

It is possible to check, by the use of Axiom or another software of computational algebra, that

$$\begin{aligned}\phi_1 = {} & (x + (-4\zeta_9^5 - 4\zeta_9^4 - 4\zeta_9^3 - 4\zeta_9^2 - 4\zeta_9)k^2) \cdot (x + (-4\zeta_9^5 - 4\zeta_9^2 + 4\zeta_9 - 4)k^2) \\ & \cdot (x + (-4\zeta_9^5 + 4\zeta_9^4 + 4\zeta_9^3 - 4\zeta_9^2 + 4)k^2) \cdot (x + (-4\zeta_9^4 + 4\zeta_9^2 - 4\zeta_9 - 4)k^2) \\ & \cdot (x + (4\zeta_9^5 - 4\zeta_9^4 + 4\zeta_9^3 - 4\zeta_9 + 4)k^2) \cdot (x + (4\zeta_9^5 - 4\zeta_9^3 + 4\zeta_9)k^2) \\ & \cdot (x + (4\zeta_9^3 + 4\zeta_9^2 + 4\zeta_9 + 4)k^2) \cdot (x + (4\zeta_9^4 - 4\zeta_9^3 + 4\zeta_9^2)k^2) \\ & \cdot (x + (4\zeta_9^5 + 4\zeta_9^4 - 4)k^2)\end{aligned}$$

and

$$\begin{aligned}\phi_2 = {} & [x + \frac{4}{3}((-\zeta_9^5 - \zeta_9^4 + 2)\sqrt[3]{3}^2 + (-2\zeta_9^5 - \zeta_9^4 - \zeta_9^2 + \zeta_9 + 3)\sqrt[3]{3} - 3\zeta_9^5 - 3\zeta_9^4 + 3)k^2] \\ & \cdot [x + \frac{4}{3}(\zeta_9^4 - \zeta_9^2 + \zeta_9 + 2)\sqrt[3]{3}^2 + (\zeta_9^5 + 2\zeta_9^4 - \zeta_9^2 + \zeta_9 + 3)\sqrt[3]{3} + 3\zeta_9^4 - 3\zeta_9^2 + 3\zeta_9 + 3)k^2] \\ & \cdot [x + \frac{4}{3}(-\zeta_9^5 + \zeta_9^4 - 2\zeta_9^3 + \zeta_9 - 2)\sqrt[3]{3}^2 + (\zeta_9^5 - \zeta_9^4 + 3\zeta_9^3 - \zeta_9^2 + \zeta_9)\sqrt[3]{3} - 3\zeta_9^5 + 3\zeta_9^2 - 3\zeta_9 + 3)k^2] \\ & \cdot [x + \frac{4}{3}(-2\zeta_9^4 + 2\zeta_9^3 - \zeta_9^2)\sqrt[3]{3}^2 + (-2\zeta_9^5 + 2\zeta_9^4 - 3\zeta_9^3 - \zeta_9^2 + \zeta_9 - 3)\sqrt[3]{3} + 3\zeta_9^5 + 3\zeta_9^2 - 3\zeta_9 + 3)k^2]\end{aligned}$$

$$\cdot[x+\frac{4}{3}((-\zeta_9^5+2\zeta_9^4-\zeta_9)\sqrt[3]{3}^2+(\zeta_9^5-\zeta_9^4-3\zeta_9^3+2\zeta_9^2+\zeta_9-3)\sqrt[3]{3}-3\zeta_9^4-3\zeta_9^2+3\zeta_9+3)k^2]$$

$$\cdot[x+\frac{4}{3}((\zeta_9^5-\zeta_9^4-2\zeta_9^3+\zeta_9^2-2)\sqrt[3]{3}^2+(-2\zeta_9^5-\zeta_9^4+3\zeta_9^3-\zeta_9^2-2\zeta_9)\sqrt[3]{3}-3\zeta_9^4-3\zeta_9^2+3\zeta_9+3)k^2]$$

$$\cdot[x+\frac{4}{3}((\zeta_9^5+\zeta_9^2-\zeta_9+2)\sqrt[3]{3}^2+(\zeta_9^5-\zeta_9^4+2\zeta_9^2-2\zeta_9+3)\sqrt[3]{3}+3\zeta_9^5+3\zeta_9^2-3\zeta_9+3)k^2]$$

$$\cdot[x+\frac{4}{3}((\zeta_9^5+\zeta_9^4+2\zeta_9^3+\zeta_9^2+\zeta_9)\sqrt[3]{3}^2+(\zeta_9^5-\zeta_9^4-3\zeta_9^3-\zeta_9^2-2\zeta_9-3)\sqrt[3]{3}-3\zeta_9^5-3\zeta_9^4+3)k^2]$$

$$\cdot[x+\frac{4}{3}\ (-2\zeta_9^3-\zeta_9^2-\zeta_9-2)\sqrt[3]{3}^2+(\zeta_9^5+2\zeta_9^4+3\zeta_9^3+2\zeta_9^2+\zeta_9)\sqrt[3]{3}-3\zeta_9^5-3\zeta_9^4+3)k^2]$$

Therefore the splitting field of $\phi_1$ is $\mathbb{Q}(\zeta_9)$ and the splitting field of $\phi_2$ is $\mathbb{Q}(\zeta_9,\sqrt[3]{3})$. We choose one root of each of these two polynomials, respectively

$$x_{1,k} := (4\zeta_9^4-4\zeta_9^2+4\zeta_9+4)k^2$$

and

$$x_{2,k} := -\frac{4}{3}((-\zeta_9^5-\zeta_9^4+2)\sqrt[3]{3}^2+(-2\zeta_9^5-\zeta_9^4-\zeta_9^2+\zeta_9+3)\sqrt[3]{3}-3\zeta_9^5-3\zeta_9^4+3)k^2.$$

By using the equation $y^2=x^3+16k^6$, we can find two ordinates $y_{1,k}$ and $y_{2,k}$, corresponding respectively to $x_{1,k}$ and $x_{2,k}$ on $\mathcal{E}_k$

$$y_{1,k} = (8\zeta_9^5+16\zeta_9^4-8\zeta_9^2+8\zeta_9+12)k^3,$$

$$y_{2,k} = \frac{4}{3}((2\zeta_9^5+8\zeta_9^4+8\zeta_9^3+10\zeta_9^2+10\zeta_9+4)\sqrt[3]{3}^2+(12\zeta_9^4+12\zeta_9^3+12\zeta_9^2+12\zeta_9+6)\sqrt[3]{3}+$$

$$+18\zeta_9^4+18\zeta_9^3+18\zeta_9^2+18\zeta_9+9)k^3.$$

The points $B_{1,k} := (x_{1,k}, y_{1,k})$ and $B_{2,k} := (x_{2,k}, y_{2,k})$ form a basis of $\mathcal{E}_k[9]$. Therefore $\mathbb{Q}(\mathcal{E}_k[9]) = \mathbb{Q}(\zeta_9,\sqrt[3]{3})$, for all $k\in\mathbb{Q}$. And we have the same Galois group $G = \mathrm{Gal}(\mathbb{Q}(\mathcal{E}_k[9])/\mathbb{Q}) = \mathrm{Gal}(\mathbb{Q}(\zeta_9,\sqrt[3]{3})/\mathbb{Q})$, for all $k\in\mathbb{Q}$. In particular $|G|=18$. Let $G_3$ be the 3-Sylow subgroup of $G$. We have $G_3 = \mathrm{Gal}(\mathbb{Q}(\zeta_9,\sqrt[3]{3})/\mathbb{Q}(\zeta_3))$. Then $G_3$ has order 9 and it is generated by the maps

$$\omega : \zeta_9 \mapsto \zeta_9^4$$

$$\tau : \sqrt[3]{3} \mapsto \zeta_3\sqrt[3]{3}.$$

Clearly $G_3 \cong (\mathbb{Z}/3\mathbb{Z})^2$.

## 4.2 Counterexamples to local-global divisibility by 9

For the curves of the family $\mathcal{E}_k$, with $k \in \mathbb{Q}$, we will prove this statement

**Theorem 4.2.1.** *There exist number fields $L$, depending on $k$, with $[L : \mathbb{Q}(\zeta_3)] \leq 2$, and points $P_k \in \mathcal{E}_k(L)$ such that $P_k \in 9\mathcal{E}_k(L_v)$ for almost all $v \in M_L$, but $P_k \notin 9\mathcal{E}_k(L)$.*

**Proof.** Since $\mathcal{E}_k[9] \cong \mathbb{Z}/9\mathbb{Z}^2$, we use the above basis $\{B_{1,k}, B_{2,k}\}$ to represent $G_3$ as a subgroup of $\mathrm{GL}_2(\mathbb{Z}/9\mathbb{Z})$. It is possible to verify that

$$B_{1,k} \overset{\omega}{\longmapsto} 7B_{1,k},$$

$$B_{2,k} \overset{\omega}{\longmapsto} 7B_{2,k},$$

$$B_{1,k} \overset{\tau}{\longmapsto} B_{1,k},$$

$$B_{2,k} \overset{\tau}{\longmapsto} 3B_{1,k} + B_{2,k}.$$

Therefore we can represent $\omega$ and $\tau$ in $\mathrm{GL}_2(\mathbb{Z}/9\mathbb{Z})$ as

$$\omega = \begin{pmatrix} 7 & 0 \\ 0 & 7 \end{pmatrix} \qquad \text{and} \qquad \tau = \begin{pmatrix} 1 & 3 \\ 0 & 1 \end{pmatrix}.$$

Let

$$\sigma(x, y) := \mathrm{I} + 3 \begin{pmatrix} 2x & y \\ 0 & 2x \end{pmatrix}, \quad \text{with} \quad x, y \in \mathbb{Z}/9\mathbb{Z}.$$

Then $\omega = \sigma(1, 0)$, $\tau = \sigma(0, 1)$ and $G_3 = \{\sigma(x, y) |\, x, y \in \mathbb{Z}/9\mathbb{Z}\}$. Consider the cocycle

$$Z_{\sigma(x,y)} = \begin{pmatrix} 3y \\ 0 \end{pmatrix}.$$

It verifies the local conditions. In fact, if we suppose

$$3 \begin{pmatrix} 2x & y \\ 0 & 2x \end{pmatrix} \begin{pmatrix} a \\ b \end{pmatrix} \equiv \begin{pmatrix} 3y \\ 0 \end{pmatrix} \pmod 9,$$

we get the system

$$\begin{cases} 2ax + by \equiv y \pmod 3 \\ 2bx \equiv 0 \pmod 3 \end{cases}$$

and it is easy to check that there exists a solution $(a, b) \in (\mathbb{Z}/3\mathbb{Z})^2$, for every choice of $(x, y) \in (\mathbb{Z}/9\mathbb{Z})^2$. Therefore $Z_{\sigma(x,y)} \in H^1_{loc}(G_3, \mathcal{E}_k[9])$. We show that $Z_{\sigma(x,y)}$ is nonzero in $H^1_{loc}(G_3, \mathcal{E}_k[9])$. Suppose

$$Z_\omega = (\omega - 1)\begin{pmatrix} a \\ b \end{pmatrix} \quad \text{and} \quad Z_\tau = (\tau - 1)\begin{pmatrix} a \\ b \end{pmatrix}, \quad \text{with} \quad \begin{pmatrix} a \\ b \end{pmatrix} \in \mathbb{Z}/9\mathbb{Z}^2.$$

Then

$$Z_\omega = \begin{pmatrix} 0 \\ 0 \end{pmatrix} = \begin{pmatrix} 6 & 0 \\ 0 & 6 \end{pmatrix}\begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} 6a & 0 \\ 0 & 6b \end{pmatrix}$$

and

$$Z_\tau = \begin{pmatrix} 3 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 & 3 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} 0 & 3b \\ 0 & 0 \end{pmatrix}.$$

We get the system

$$\begin{cases} 6a \equiv 0 \pmod 9 \\ 6b \equiv 0 \pmod 9 \\ 3b \equiv 3 \pmod 9 \end{cases}$$

that has no solutions. Therefore we will use Theorem 1.1.5 and Proposition 1.1.6 to find counterexamples to local-global divisibility by 9. Let $K := \mathbb{Q}(\mathcal{E}_k[9]) = \mathbb{Q}(\zeta_9, \sqrt[3]{3})$ and let $L \subsetneq F$ be finite extensions of $\mathbb{Q}(\zeta_3)$, depending on $k$ too, but disjoint from $K$ over $\mathbb{Q}(\zeta_3)$, for all choices of that parameter. For every rational $k$ we will find a point $D_k \in \mathcal{E}_k(F)$, but $D_k \notin \mathcal{E}_k(L)$, satisfying the equality

$$D_k^\sigma - D_k = Z_\sigma, \tag{4.2.1}$$

for all $\sigma \in G_3$. Then we will show that the point $P_k := 9D$ lies in $\mathcal{E}_k(L)$. Since we take $\mathbb{Q}(\zeta_3)$ as base field, the group $G_3$ is the whole Galois group of the extension $K/\mathbb{Q}(\zeta_3)$. Therefore we can repeat the same arguments of the proof of Theorem 1.1.5, with $G_3$ as Galois group, identified with $\mathrm{Gal}(LK/L)$. In this way, we can prove that the point $P_k$ is divisible by 9 over $L_w$, for all places $w$ of $L$ unramified in $LK$, but not divisible by 9 over $L$.

Let $\overline{\mathbb{Q}(\zeta_3)}$ be the algebraic closure of $\mathbb{Q}(\zeta_3)$. Suppose there exists a point $D_k \in \overline{\mathbb{Q}(\zeta_3)}$ satisfying 4.2.1, for all $\sigma \in G_3$. Since $Z_\omega$ is the zero vector, we have $D_k^\omega = D_k$. Therefore the coordinates of $D_k$ lie in $\overline{\mathbb{Q}(\zeta_3)}^\omega$, the subfield of $\overline{\mathbb{Q}(\zeta_3)}$ fixed by $\omega$. Furthermore $D_k$ satisfies the equation $D_k^\tau - D_k = Z_\tau$. We want to use also this relation, so we suppose

$$D_k = \begin{pmatrix} u_k \\ v_k \end{pmatrix}, \quad \text{with } u_k = r_0 + s_0\zeta_3 + (r_1 + s_1\zeta_3)\sqrt[3]{3} + (r_2 + s_2\zeta_3)\sqrt[3]{3}^2,$$
$$v_k = t_0 + w_0\zeta_3 + (t_1 + w_1\zeta_3)\sqrt[3]{3} + (t_2 + w_2\zeta_3)\sqrt[3]{3}^2,$$

where $r_i,\ s_i, t_i, w_i$ are in $\overline{\mathbb{Q}(\zeta_3)}^H$, the subfield of $\overline{\mathbb{Q}(\zeta_3)}$ fixed by $H := G/ < \tau >$, and clearly depend on $k$, for all $i \in \{0, 1, 2\}$. Therefore

$$u_k^\tau = r_0 + s_0\zeta_3 + (r_1\zeta_3 - s_1 - s_1\zeta_3)\sqrt[3]{3} + (-r_2 - r_2\zeta_3 + s_2)\sqrt[3]{3}^2,$$

$$v_k^\tau = t_0 + w_0\zeta_3 + (t_1\zeta_3 - w_1 - w_1\zeta_3)\sqrt[3]{3} + (-t_2 - t_2\zeta_3 + w_2)\sqrt[3]{3}^2.$$

With respect to the basis $\{B_{1,k}, B_{2,k}\}$, the point $Z_\tau$ can be written as

$$Z_\tau = \begin{pmatrix} 3 \\ 0 \end{pmatrix},$$

then corresponds to $3B_{1,k} = (0, 4k^3)$. We denote this point by $A = (x_a, y_a) := (0, 4k^3)$. Let $\lambda$ be the slope of the line passing through $A$ and $D_k$. Then $\lambda = \frac{v_k - y_a}{u_k - x_a} = \frac{v_k - 4k^3}{u_k}$. By using the group law on an elliptic curve, we get the system

$$\begin{cases} \lambda^2 = u_k + u_k^\tau + x_a = u_k + u_k^\tau \\ \\ v_k^\tau = \lambda(x_a - u_k^\tau) - y_a = -\lambda u_k - 4k^3 \end{cases} \tag{4.2.2}$$

The first equation says

$$(v_k - 4k^3)^2/u_k^2 = u_k + u_k^\tau, \quad i.e. \quad (v_k - 4k^3)^2 = u_k^2(u_k + u_k^\tau) = u_k^3 + u_k^2 u_k^\tau.$$

Since $D_k \in \mathcal{E}_k$, we have the relation $v_k^2 = u_k^3 + 16k^6$ and therefore $(v_k - 4k^3)^2 = v_k^2 - 8k^3 v_k + 16k^6 = u_k^3 - 8k^3 v_k + 32k^6$. Then

$$8k^3 v_k = -u_k^2 u_k^\tau + 32k^6 \tag{4.2.3}$$

The second equation says $\lambda = -\frac{v_k^\tau + y_a}{u_k^\tau - x_a} = -\frac{v_k^\tau + 4k^3}{u_k^\tau}$. Then $\frac{v_k - 4k^3}{u_k} = -\frac{v_k^\tau + 4k^3}{u_k^\tau}$ and we have

$$u_k^\tau(v_k - 4k^3) = u_k(v_k^\tau + 4k^3) \tag{4.2.4}$$

By substituting $u_k = r_0 + s_0\zeta_3 + (r_1 + s_1\zeta_3)\sqrt[3]{3} + (r_2 + s_2\zeta_3)\sqrt[3]{3}^2$ and $v_k = t_0 + w_0\zeta_3 + (t_1 + w_1\zeta_3)\sqrt[3]{3} + (t_2 + w_2\zeta_3)\sqrt[3]{3}^2$ in the equation 4.2.3, we can find the equivalent system of equations

$$\begin{cases}
t_0 = 9r_2^3 - 27s_2r_2^2 + 9s_1r_1^2 - 9s_1^2r_1 - r_0^3 + 3s_0^2r_0 + 9s_2^3 - s_0^3 + 32 \\
w_0 = 9r_2^3 - 27s_2^2r_2 - 3r_1^3 + 9s_1r_1^2 - 3s_0r_0^2 + 3s_0^2r_0 + 9s_2^3 - 3s_1^3 \\
t_1 = 3r_0r_2^2 - 6s_0r_2^2 + 3r_1^2r_2 + 6s_1r_1r_2 - 12s_2r_0r_2 + 6s_0r_2r_2 - 6s_1^2r_2 + 3s_2r_1^2 \\
\quad -2r_0^2r_1 + 2s_0r_0r_1 - 12s_1s_2r_1 + s_0^2r_1 + s_1r_0^2 + 3s_2^2r_0 + 2s_0s_1r_0 + 3s_0s_2^2 \\
\quad +3s_1^2s_2 - 2s_0^2s_1 \\
w_1 = 6r_0r_2^2 - 3r_0r_2^2 - 3r_1^2r_2 + 12s_1r_1r_2 - 6s_2r_0r_2 - 6s_0s_2r_2 - 3s_1^2r_2 + 6s_2r_1^2 \\
\quad -r_0^2r_1 - 2s_0r_0r_1 - 6s_1s_2r_1 + 2s_0^2r_1 - s_1r_0^2 - 3s_2^2r_0 + 4s_0s_1r_0 + 6s_0s_2^2 \\
\quad -3s_1^2s_2 - s_0^2s_1 \\
t_2 = 6r_1r_2^2 - 3s_1r_2^2 - 6s_2r_1r_2 - r_0^2r_2 - 2s_0r_0r_2 - 6s_1s_2r_2 + 2s_0^2r_2 - r_0r_1^2 + 2s_0r_1^2 \\
\quad +4s_1r_0r_1 - 3s_2^2r_1 - 2s_0s_1r_1 - s_2r_0^2 + 4s_0s_2r_0 - s_1^2r_0 + 6s_1s_2^2 - s_0^2s_2 - s_0s_1^2 \\
w_2 = 3r_1r_2^2 + 3s_1r_2^2 + 6s_2r_1r_2 + r_0^2r_2 - 4s_0r_0r_2 - 12s_1s_2r_2 + s_0^2r_2 - 2r_0r_1^2 + s_0r_1^2 \\
\quad +2s_1r_0r_1 - 6s_2^2r_1 + 2s_0s_1r_1 - 2s_2r_0^2 + 2s_0s_2r_0 + s_1^2r_0 + 3s_1s_2^2 + s_0^2s_2 - 2s_0s_1^2
\end{cases}$$

In the same way we can to find a system of six equations in the variables $r_i, s_i, t_i, w_i$, with $i \in \{0, 1, 2\}$, equivalent to the equation 4.2.4. Therefore we get a system of 12 equations in the 12 variables $r_i, s_i, t_i, w_i$, equivalent to the system 4.2.2. It is possible to find one of its solutions, by using a software of computational algebra. We used the software Axiom to find the following one.

Let $l_k = \sqrt[3]{-8k^3\sqrt{16k^3+1} + 32k^6 + k^3}$. Its minimal polynomial over $\mathbb{Q}(\zeta_3)$ is $p := x^6 + (-64k^6 - 2k^3)x^3 + k^6$. A solution of the system of 12 equations is

$$r_0 = k; \quad r_1 = -27r_2^5 + 198r_2^2 = \frac{-l_k^5 + (64k^6 + 2k^3)l_k^2}{k^4\sqrt[3]{3}}; \quad r_2 = \frac{l_k}{\sqrt[3]{3}^2};$$

$$s_0 = k; \quad s_1 = u_1; \quad s_2 = r_2.$$

Therefore a solution of the system 4.2.2 is

$$u_k = \frac{(-l_k^5 + (64k^6 + 2k^3)l_k^2 + k^4 l_k + k^5)\zeta_3 - l_k^5 + (64k^6 + 2k^3)l_k + k^4 l_k + k^5}{k^4},$$

$$\begin{aligned} v_k &= 4k^3 - \frac{1}{8k^3}u_k^2 u_k^\tau = \\ &= \frac{(-2l_k^5 - 2kl_k^4 - 2k^2 l_k^3 + (128k^6 + 2k^3)l_k^2 + (128k^7 + 2k^4)l_k + 64k^8 + 2k^5)}{8k^5}\zeta_3 \\ &\quad + \frac{-l_k^5 - kl_k^4 - k^2 l_k^3 + (64k^6 + k^3)l_k^2 + (64k^7 + k^4)l_k + 32k^8 + k^5}{8k^5}. \end{aligned}$$

The point $D_k$ lies on $\mathcal{E}_k(F)$, where $F$ is the field $\mathbb{Q}(l_k, \zeta_3)$ of degree at most 6 over $\mathbb{Q}(\zeta_3)$. Clearly $F$ depend on $k$, but we do not write that subscript in the case of fields, in order to avoid confusion with completions. Let $h_k := l_k^3 = -8k^3\sqrt{16k^3+1} + 32k^6 + k^3$. The point $3D_k := (u_{3,k}, v_{3,k})$ lies on $\mathcal{E}_k(L)$, where $L$ is the field $\mathbb{Q}(h, \zeta_3) = \mathbb{Q}(\sqrt{16k^3+1}, \zeta_3)$ of degree at most 2 over $\mathbb{Q}(\zeta_3)$. In fact it is possible to check that

$$u_{3,k} = \frac{(-64k^4 - k)}{3\zeta_3},$$

$$\begin{aligned} v_{3,k} = &\frac{(-128k^6 + k^3)h_k + 4096k^6 + 96k^3 - 1}{36k^3}\,\zeta_3 \\ &+ \frac{(-128k^6 + k^3)h_k + 4096k^6 + 96k^3 - 1}{36k^3}. \end{aligned}$$

Then the point $P_k := 9D_k = 3(3D_k)$ lies in $\mathcal{E}_k(L)$ too. Let $P_k := (u_{9,k}, v_{9,k})$. The coordinates $u_{9,k}$ and $v_{9,k}$ have very long expressions in terms of $k$, but they become really easier for every numerical choice of that parameter. The abscissas $u_{9,k}$ is a fraction with the following numerator $n_{1,k}$ and denominator $d_{1,k}$

$$\begin{aligned} n_{1,k} = &- 18014398509481984k^{28} - 2533274790395904k^{25} - 300826381359513 6k^{22} \\ &- 272953761595392k^{19} - 12920335368192k^{16} - 329621962752k^{13} \\ &+ 869793792k^{10} - 25030656k^7 - 42048k^4 - k, \end{aligned}$$

$$\begin{aligned} d_{1,k} =&(7599824371187712k^{24} + 949978046398464k^{21} - 48241072668672k^{18} \\ &- 6204080259072k^{15} + 117323071488k^{12} + 6893862912k^{9} + 53858304k^{6} \\ &- 79488k^{3} + 27)\,\zeta_3. \end{aligned}$$

And the ordinate $v_{9,k}$ is a fraction with the following numerator $n_{2,k}$ and denominator $d_{2,k}$

$$\begin{aligned} n_{2,k} =\ & 773712524553362671811952 64k^{48} + 18738350204026752207945728k^{45} \\ & -260485735195089629987471 36k^{42} - 53526548343801531733114 88k^{39} \\ & -816515150463633524260864k^{36} - 75787727450895313534976k^{33} \\ & -356561804447944015872 0k^{30} - 852512937665888256 00k^{27} \\ & -131546684402643763 2k^{24} - 20578337218887680k^{21} \\ & +172867702489088k^{18} + 576131694592k^{15} \\ & +3002884096k^{12} + 755072k^{9} - 8k^{6} \end{aligned}$$

$$d_{2,k} = 2(f(k)h + g(k))\,\zeta_3 + f(k)h + g(k), \quad \text{with}$$

$$\begin{aligned} f(k) =\ & 382511685112441262309376k^{36} + 71720940958582736683008k^{33} \\ & -140079962809731907584 0k^{30} - 74271563614743271833 6k^{27} \\ & -533507670857377382 4k^{24} + 25328789662099046 40k^{21} \\ & 21374506043965440k^{18} - 2150235648294912k^{15} \\ & -44238045708288k^{12} - 196560027648k^{9} \\ & +505626624k^{6} - 357696k^{3} + 81, \end{aligned}$$

$$g(k) = -1224037392359812039390003 2k^{42} - 267758179578708883616563 2k^{39}$$
$$-2689535285946852625612 8k^{36} + 251676999848151660625 92k^{33}$$
$$9134380908217934807 04k^{30} - 757170502101431746 56k^{27}$$
$$-3216863159616798720k^{24} + 4743034701471744k^{21}$$
$$+3565853110960128k^{18} + 505279665930 24k^{15}$$
$$+180379975680k^{12} - 494180352k^9 + 355104k^6 - 81k^3.$$

By the arguments of the proof of Theorem 1.1.5, with $G_3$ as Galois group, identified with $\mathrm{Gal}(LK/L)$, the point $P_k$ is locally divisible by 9 almost everywhere, but not globally, over $L$. □

To produce an easier numerical example, we now suppose $k = 1$. To get a lighter notation, we will omit that subscript from now on. Then we have the curve $\mathcal{E} : y^2 = x^3 + 16$, the polynomial $p := x^6 - 66x^3 + 1$ and one of its solution $l = \sqrt[3]{-8\sqrt{17} + 33}$. The point $D$ has coordinates

$$u = (-l^5 + 66l^2 + l + 1)\zeta_3 - l^5 + 66l + l_k + 1,$$
$$v = \frac{-l^5 - l^4 - l^3 + 65l^2 + 65l + 32 + 1}{4}\,\zeta_3 + \frac{-l^5 - l^4 - l^3 + 65l^2 + 65l + 32 + 1}{8}.$$

As above, let $h = l^3$. Therefore the point $3D$ has coordinates

$$u_3 = -\frac{65}{3\zeta_3} = \frac{65\zeta_3 + 65}{3},$$
$$v_3 = \frac{-127h + 4191}{36}\,\zeta_3 + \frac{-127h + 4191}{36},$$

and the point $9D = P = (u_9, v_9)$ has coordinates

$$u_9 = -\frac{23842139987678273\zeta_3 + 23842139987678273}{8495481535371675},$$

$$v_9 = \frac{4692089648702161319323 51h - 154838958407171323537675 83}{5425035933466478142391500}\,\zeta_3$$

$$+ \frac{4692089648702161319323 51h - 154838958407171323537675 83}{1085007186693295628478300 0}.$$

Then $P$ lies in $\mathcal{E}_k(L)$, where $L := \mathbb{Q}(h, \zeta_3) = \mathbb{Q}(\sqrt{17}, \zeta_3)$, but $D$ don't lie in $\mathcal{E}_k(L)$. It lies on $\mathcal{E}_k(F)$, where $F := \mathbb{Q}(l, \zeta_3) = \mathbb{Q}(\sqrt[3]{-8\sqrt{17}+33}, \zeta_3)$. Therefore, the 9-divisors of $P$ lie in $\mathcal{E}_k(FK) = \mathcal{E}_k(\mathbb{Q}(l, \zeta_9, \sqrt[3]{3}))$. In Appendix C, we will show how it is possible to verify directly, by using Axiom, that no one of them lies in $L$, i. e., that $P$ is not divisible by 9 over $L$.

## 4.3 A counterexample when $|G_3| = 27$

We give another counterexample to local-global divisibility by 9, for an elliptic curve of the family $\mathcal{F}_{\beta,h}$, such that $G_3 \cong (\mathbb{Z}/3\mathbb{Z})^3$.

Let

$$\mathcal{E}: \quad y^2 = x^3 + 189x + 702.$$

We observe that $\mathcal{E}$ is a curve in the family $\mathcal{F}_{\beta,h}$, obtained by choosing $\beta = 12$ and $h = 6$ or $h = -6$. By using the method shown in 4.2, it is possible to verify that $\mathcal{E}[9]$ is generated by the points $B_1 = (x_1, y_1)$ and $B_2 = (x_2, y_2)$ of coordinates

$$x_1 = -12\sqrt[3]{2} - 9,$$

$$y_1 = (48\zeta_3 + 24)\sqrt[3]{2}^2 + (24\zeta_3 + 12)\sqrt[3]{2} + 48\zeta_3 + 24,$$

$$x_2 = (4\zeta_9^5 + 4\zeta_9^4 + 4)\sqrt[3]{3}^2 - (4\zeta_9^5 - 4\zeta_9^4 + 8\zeta_9^2 - 8\zeta_9 - 12)\sqrt[3]{3} + 12\zeta_9^5 + 12\zeta_9^4 + 3,$$

$$y_2 = (36\zeta_9^5 + 60\zeta_9^4 - 24\zeta_9^2 + 24\zeta_9 + 12)\sqrt[3]{3}^2 + (12\zeta_9^5 + 60\zeta_9^4 - 48\zeta_9^2 + 48\zeta_9 + 36)\sqrt[3]{3}$$

$$- 36\zeta_9^5 + 36\zeta_9^4 - 72\zeta_9^2 + 72\zeta_9 + 108.$$

Then $\mathbb{Q}(\mathcal{E}[9]) = \mathbb{Q}(\zeta_9, \sqrt[3]{2}, \sqrt[3]{3}) = \mathbb{Q}(\sqrt[3]{-1+\sqrt{-3}}, \sqrt[3]{2}, \sqrt[3]{3})$. Clearly $[\mathbb{Q}(\mathcal{E}[9]) : \mathbb{Q}] = 54$. Let $G := \mathrm{Gal}(\mathbb{Q}(\mathcal{E}[9])/\mathbb{Q})$ and let $G_3$ be its 3-Sylow subgroup. Then $G_3 = \mathrm{Gal}(\mathbb{Q}(\mathcal{E}[9])/\mathbb{Q}(\zeta_3))$ and it is generated by

$$\omega : \zeta_9 \mapsto \zeta_9^4,$$

$$\tau_1 : \sqrt[3]{3} \mapsto \zeta_3\sqrt[3]{3},$$

$$\tau_2 : \sqrt[3]{2} \mapsto \zeta_3\sqrt[3]{2}.$$

Clearly $G_3 \cong (\mathbb{Z}/3\mathbb{Z})^3$. As in 4.2, we represent $\omega, \tau_1$ and $\tau_2$ in $\mathrm{GL}_2(\mathbb{Z}/9\mathbb{Z})$ with respect to the above basis $\{B_1, B_2\}$. It is possible to check

$$\omega = \begin{pmatrix} 1 & 0 \\ 0 & 4 \end{pmatrix}, \qquad \tau_1 = \begin{pmatrix} 1 & 6 \\ 0 & 1 \end{pmatrix}, \qquad \tau_2 = \begin{pmatrix} 1 & 0 \\ 3 & 7 \end{pmatrix}.$$

Let $$\sigma(x,y,z) := \mathrm{I} + \begin{pmatrix} 0 & 6x \\ 3y & 6y+3z \end{pmatrix} = \mathrm{I} + 3\begin{pmatrix} 0 & 2x \\ y & 2y+z \end{pmatrix}, \quad \text{with} \quad x,y,z \in \mathbb{Z}/9\mathbb{Z}.$$

Then $\tau_1 = \sigma(1,0,0)$, $\tau_2 = \sigma(0,1,0)$, $\omega = \sigma(0,0,1)$ and $G_3 = \{\sigma(x,y,z) | x,y,z \in \mathbb{Z}/9\mathbb{Z}\}$. Consider the cocycle

$$Z_{\sigma(x,y,z)} = \begin{pmatrix} 3x \\ 0 \end{pmatrix}.$$

It verifies the local conditions. In fact, if we suppose

$$3\begin{pmatrix} 0 & 2x \\ y & 2y+z \end{pmatrix}\begin{pmatrix} a \\ b \end{pmatrix} \equiv \begin{pmatrix} 3x \\ 0 \end{pmatrix} \pmod 9,$$

we get the system

$$\begin{cases} 2bx \equiv x \pmod 3 \\ ay + 2by + bz \equiv 0 \pmod 3 \end{cases}$$

and it is easy to verify that there exists a solution $(a,b) \in (\mathbb{Z}/3\mathbb{Z})^2$ for every choice of $(x,y,z) \in (\mathbb{Z}/9\mathbb{Z})^3$. Therefore $Z_{\sigma(x,y,z)} \in H^1_{loc}(G_3, \mathcal{E}_k[9])$. We show that $Z_{\sigma(x,y,z)}$ represents a nonzero element in $H^1_{loc}(G_3, \mathcal{E}_k[9])$. Suppose

$$Z_{\tau_1} = (\tau_1 - 1)\begin{pmatrix} a \\ b \end{pmatrix} \quad \text{and} \quad Z_\omega = (\omega - 1)\begin{pmatrix} a \\ b \end{pmatrix}, \quad \text{with} \quad \begin{pmatrix} a \\ b \end{pmatrix} \in \mathbb{Z}/9\mathbb{Z}^2.$$

Then

$$Z_{\tau_1} = \begin{pmatrix} 3 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 & 6 \\ 0 & 3 \end{pmatrix}\begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} 0 & 6b \\ 0 & 0 \end{pmatrix}$$

and

$$Z_\omega = \begin{pmatrix} 0 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 3 \end{pmatrix}\begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 3b \end{pmatrix}.$$

We get the system

$$\begin{cases} 6b \equiv 3 \pmod 9 \\ 3b \equiv 0 \pmod 9 \end{cases}$$

that has no solutions. Again, we will use Theorem 1.1.5 and Proposition 1.1.6 to find a point $P$ on $\mathcal{E}$ that gives a counterexample to local-global divisibility by 9. Let $K := \mathbb{Q}(\mathcal{E}[9]) = \mathbb{Q}(\zeta_9, \sqrt[3]{2}, \sqrt[3]{3})$ and let $L \subsetneq F$ be finite extensions of $\mathbb{Q}(\zeta_3)$, disjoint from $K$ over $\mathbb{Q}(\zeta_3)$. As in 4.2, we will find a point $D \in \mathcal{E}(F)$, but $D \notin \mathcal{E}(L)$, satisfying $D^\sigma - D = Z_\sigma$, for all $\sigma \in G_3$. We will show that the point $P := 9D$ lies in $\mathcal{E}(L)$. For a such point we can apply the arguments used in the proof of Theorem 1.1.5, with $G_3$ as Galois group, identified with $\mathrm{Gal}(LK/L)$. In this way, we may prove that $P$ is divisible by 9 over $L_w$, for all places $w \in L$, unramified in $LK$, but $P$ is not divisible by 9 over $L$.

We suppose there exists a point $D$ on $\mathcal{E}$, satisfying $Z_\sigma = D^\sigma - D$, for all $\sigma \in G_3$. Again, let $\overline{\mathbb{Q}(\zeta_3)}$ be the algebraic closure of $\mathbb{Q}(\zeta_3)$. Since $Z_\omega$ and $Z_{\tau_2}$ are the zero vector, we have $D^\omega = D$ and $D^{\tau_2} = D$. Therefore the coordinates of $D$ lie in $\overline{\mathbb{Q}(\zeta_3)}^{<\omega,\tau_2>}$, the subfield of $\overline{\mathbb{Q}(\zeta_3)}$ fixed by $\omega$ and $\tau_2$. Furthermore, by hypothesis, the point $D$ satisfies the equation $D^{\tau_1} - D = Z_{\tau_1}$. Since we want to use this information, we suppose

$$D_k = \begin{pmatrix} u_k \\ v_k \end{pmatrix}, \quad \text{with } u_k = r_0 + s_0\zeta_3 + (r_1 + s_1\zeta_3)\sqrt[3]{3} + (r_2 + s_2\zeta_3)\sqrt[3]{3}^2,$$
$$v_k = t_0 + w_0\zeta_3 + (t_1 + w_1\zeta_3)\sqrt[3]{3} + (t_2 + w_2\zeta_3)\sqrt[3]{3}^2,$$

where $r_i,\ s_i, t_i, w_i$ are in $\overline{\mathbb{Q}(\zeta_3)}^H$, the subfield of $\overline{\mathbb{Q}(\zeta_3)}$ fixed by $H := G/ < \tau_1 >$. We have

$$u^{\tau_1} = r_0 + s_0\zeta_3 + (r_1 + s_1\zeta_3)\zeta_3\sqrt[3]{3} + (r_2 + s_2\zeta_3)\zeta_3^2\sqrt[3]{3}^2$$

$$= r_0 + s_0\zeta_3 + (r_1\zeta_3 - s_1 - s_1\zeta_3)\sqrt[3]{3} + (-r_2 - r_2\zeta_3 + s_2)\sqrt[3]{3}^2,$$

$$v^{\tau_1} = t_0 + w_0\zeta_3 + (t_1 + w_1\zeta_3)\sqrt[3]{3} + (t_2 + w_2\zeta_3)\sqrt[3]{3}^2$$

$$= t_0 + w_0\zeta_3 + (t_1\zeta_3 - w_1 - w_1\zeta_3)\sqrt[3]{3} + (-t_2 - t_2\zeta_3 + w_2)\sqrt[3]{3}^2.$$

With respect to the basis $\{B_1, B_2\}$, the cocycle $Z_{\tau_1}$ can be written as

$$Z_{\tau_1} = \begin{pmatrix} 3 \\ 0 \end{pmatrix},$$

then it corresponds to $3B_1 = (-9, 48\zeta_3 + 24)$. Let $A = (x_a, y_a) := (-9, 48\zeta_3 + 24)$ and let $\lambda$ be the slope of the line passing trough $A$ and $D$. Then $\lambda = (v - y_a)/(u - x_a) = (v - 48\zeta_3 - 24)/(u + 9)$. By using the group law on an elliptic curve, we get the system

$$\begin{cases} \lambda^2 = u + u^{\tau_1} + x_a = u + u^{\tau} - 9 \\ \\ v^{\tau_1} = \lambda(x_a - u^{\tau_1}) - y_a = -\lambda(u - 9) - 48\zeta_3 - 24 \end{cases} \tag{4.3.1}$$

The first equation says $(v - 48\zeta_3 - 24)^2/(u + 9)^2 = u + u^{\tau_1} - 9$, i. e.

$$\begin{aligned}(v - 48\zeta_3 - 24)^2 &= (u + 9)^2(u + u^{\tau_1} - 9) \\ &= u^3 + (u^{\tau_1} + 9)u^2 + (18u^{\tau_1} - 81)u + 81u^{\tau_1} - 729.\end{aligned}$$

On the other hand, since $D \in \mathcal{E}$, we have the relation $v^2 = u^3 + 189u + 702$ and therefore

$$\begin{aligned}(v - 48\zeta_3 - 24)^2 &= v^2 - 2(48\zeta_3 + 24)v + (48\zeta_3 + 24)^2 \\ &= u^3 + 189u + 702 - 2(48\zeta_3 + 24)v + (48\zeta_3 + 24)^2.\end{aligned}$$

The first equation in the system above becomes

$$(-96z3 - 48)v = (u^{\tau_1} + 9)u^2(18u^{\tau_1} - 270)u + 81u^{\tau_1} + 297. \tag{4.3.2}$$

The second equation in the system says

$$\lambda = -\frac{v^{\tau_1} + y_a}{u^{\tau_1} - x_a} = -\frac{v^{\tau_1} + 48\zeta_3 + 24}{u^{\tau} + 9}.$$

Then $(v_k - 48\zeta_3 - 24)/(u + 9) = (v^{\tau_1} + 48\zeta_3 + 24)/(u^{\tau_1} + 9)$ and we have

$$(u^{\tau} + 9)(v - 48\zeta_3 - 24) = (u + 9)(v^{\tau_1} + 48\zeta_3 + 24). \tag{4.3.3}$$

As in 4.2, by substituting $u = r_0 + s_0\zeta_3 + (r_1 + s_1\zeta_3)\sqrt[3]{3} + (r_2 + s_2\zeta_3)\sqrt[3]{3}^2$ and $v = t_0 + w_0\zeta_3 + (t_1 + w_1\zeta_3)\sqrt[3]{3} + (t_2 + w_2\zeta_3)\sqrt[3]{3}^2$ in the equations 4.3.2 and 4.3.3, it is possible to find a system of 12 equations in the 12 variables $r_i, s_i, t_i, w_i$, equivalent to the system 4.3.1. Again, we used the software Axiom to find a solution of that system.

Let $t = \sqrt[3]{-64\sqrt{3} - 11}$. Its minimal polynomial over $\mathbb{Q}(\zeta_3)$ is $p := x^6 + 22x^3 - 12167$. A solution of the system of 12 equations is

$$r_0 = 0; \qquad r_1 = 0; \qquad r_2 = l\sqrt[3]{3};$$

$$s_0 = 0; \qquad s_1 = \frac{t^5 + 22t^2}{529}\sqrt[3]{3}^2; \qquad s_2 = l\sqrt[3]{3}.$$

Then a solution of the system 4.3.1 is

$$u = r_0 + s_0\zeta_3 + (r_1 + s_1\zeta_3)\sqrt[3]{3} + (r_2 + s_2\zeta_3)\sqrt[3]{3}^2$$

$$= \frac{(3t^5 + 66t^2 + 1587t)\zeta_3 + 1587t}{529},$$

$$v = -\frac{(u^{\tau_1} + 9)u^2(18u^{\tau_1} - 270)u + 81u^{\tau_1} + 297}{96\zeta_3 + 48}$$

$$= \frac{(63t^5 + 621t^4 + 15669t^2 - 19665t)\zeta_3 + 621t^4 - 4761t^3 - 19665t - 52371}{8464}.$$

The point $D$ lies on $\mathcal{E}(F)$, where $F$ is the field $\mathbb{Q}(t, \zeta_3)$ of degree 6 over $\mathbb{Q}(\zeta_3)$. Let $w := t^3 = -64\sqrt{3} - 11$ and let $L$ be the field $\mathbb{Q}(w, \zeta_3) = \mathbb{Q}(\sqrt{3}, i)$ of degree 2 over $\mathbb{Q}(\zeta_3)$. The point $3D := (u_3, v_3)$ lies in $\mathcal{E}(L)$, in fact

$$u_3 = 114, \qquad v_{3,k} = \frac{-177w - 1947}{16}.$$

Then the point $P := 9D = 3(3D) = (u_9, v_9)$ lies in $\mathcal{E}(L)$ too. We have

$$u_9 = \frac{129910025559718}{13862198606763},$$

$$v_9 = \frac{-7407986982750875742 23w - 8148785681025963316453}{1430305422763827379536}.$$

By the arguments of the proof of Theorem 1.1.5, with $G_3$ as Galois group, identified with $\mathrm{Gal}(LK/L)$, the point $P$ is locally divisible by 9 almost everywhere, but not globally, over $L$.

# Appendix A

# Direct computation when $q = 2^2$ Part One

We will found the condition appearing in 2.1 for $\alpha, \beta$, and $\gamma$, to have that the group $G$, considered in the cases when $n = 3$, is the Galois group $\mathrm{Gal}(\mathbb{Q}(\mathcal{E}[4])/\mathbb{Q})$.

## A.1 Conditions about $\alpha, \beta, \gamma, \delta$ when $|G| = 8$

Let $\alpha, \beta, \gamma, \delta$ be as in Chapter 2 and let $\mathcal{E} : y^2 = (x-\alpha)(x-\beta)(x-\gamma)$. Let $G$ be the group of order 8 found in 2.1

$$G =< \sigma_1, \sigma_2, \sigma_3 >, \qquad \text{with} \quad \sigma_1 = \begin{pmatrix} -1 & 0 \\ 2 & -1 \end{pmatrix}, \sigma_2 = \begin{pmatrix} 1 & 2 \\ 2 & -1 \end{pmatrix},$$

$$\sigma_3 = \begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix}.$$

We consider the field $\mathbb{Q}(\mathcal{E}[4]) = \mathbb{Q}(\sqrt{-1}, \sqrt{\alpha-\beta}, \sqrt{\beta-\gamma}, \sqrt{\alpha-\gamma})$. We have to require that $\mathrm{Gal}(\mathbb{Q}(\mathcal{E}[4])/\mathbb{Q})$ corresponds to $G$. For a generic point $Q \in \mathcal{E}$, let $(x_Q, y_Q)$ be its coordinates and for two generic points $Q_1, Q_2 \in \mathcal{E}$, let $\lambda_{Q_1+Q_2}$ be the slope of the line passing through $Q_1$ and $Q_2$. We consider a basis $A', B' \in \mathcal{E}[4]$ to represent $\mathrm{Gal}(\mathbb{Q}(\mathcal{E}[4])/\mathbb{Q})$ as a subgroup of $\mathrm{GL}_2(\mathbb{Z}/4\mathbb{Z})$. We choose $A', B'$ such that $A' = 2A$ and $B' = 2B$, where $A = (\alpha, 0)$ and $B = (\beta, 0)$. Specifically, for some given determinations of the square roots, we may have $A' = (\alpha + \sqrt{(\alpha-\beta)(\alpha-\gamma)}, (\alpha-\beta)\sqrt{\alpha-\gamma} + (\alpha-\gamma)\sqrt{\alpha-\beta})$ and $B' = (\beta + \sqrt{(\beta-\alpha)(\beta-\gamma)}, (\beta-\gamma)\sqrt{\beta-\alpha} + (\beta-\alpha)\sqrt{\beta-\gamma})$.

We require that the two columns of $\sigma_1$ are $\sigma_1(A')$ and $\sigma_1(B')$, i.e.

*i*) $\sigma_1(A') = -A' + 2B' = -A' + B$,

*ii*) $\sigma_1(B') = -B'$.

From $ii$) it follows immediately

$\sigma_1(\beta + \sqrt{(\beta-\alpha)(\beta-\gamma)}) = \beta + \sqrt{(\beta-\alpha)(\beta-\gamma)}$,

$\sigma_1((\beta-\gamma)\sqrt{(\beta-\alpha)} + (\beta-\alpha)\sqrt{(\beta-\gamma)}) = -(\beta-\gamma)\sqrt{(\beta-\alpha)} - (\beta-\alpha)\sqrt{(\beta-\gamma)}$.

Since $\alpha, \beta, \gamma$ are rational numbers, we have

**1)** $\sigma_1(\sqrt{\beta-\alpha}) = -\sqrt{\beta-\alpha}$,

**2)** $\sigma_1(\sqrt{\beta-\gamma}) = -\sqrt{\beta-\gamma}$.

Now we analyze $i$). We calculate the coordinates of the point $-A' + B$:

$$\lambda_{B-A'} = \frac{(\alpha-\beta)\sqrt{\alpha-\gamma}+(\alpha-\gamma)\sqrt{\alpha-\beta}}{\beta-\alpha-\sqrt{(\alpha-\beta)(\alpha-\gamma)}} = \frac{(\alpha-\beta)\sqrt{\alpha-\gamma}+(\alpha-\gamma)\sqrt{\alpha-\beta}}{-(\alpha-\beta)-\sqrt{(\alpha-\beta)(\alpha-\gamma)}}$$

$$\lambda^2_{B-A'} = \frac{(\alpha-\beta)^2(\alpha-\gamma)+(\alpha-\beta)(\alpha-\gamma)^2+2(\alpha-\beta)(\alpha-\gamma)\sqrt{(\alpha-\beta)(\alpha-\gamma)}}{(\alpha-\beta)^2+(\alpha-\beta)(\alpha-\gamma)+2(\alpha-\beta)\sqrt{(\alpha-\beta)(\alpha-\gamma)}} = \alpha - \gamma,$$

$$\begin{aligned} x_{B-A'} &= \lambda^2_{B-A'} - x_B - x_{-A'} = \alpha - \gamma - \beta - \alpha - \sqrt{(\alpha-\beta)(\alpha-\gamma)} \\ &= \alpha - \sqrt{(\alpha-\beta)(\alpha-\gamma)}. \end{aligned}$$

The last equality follows from $\alpha + \beta + \gamma = 0$. The ordinate of the point $B - A'$ is

$$\begin{aligned} y_{B-A'} &= \lambda_{B-A'}(x_B - x_{B-A'}) - y_B \\ &= \frac{(\alpha-\beta)\sqrt{\alpha-\gamma}+(\alpha-\gamma)\sqrt{\alpha-\beta}}{-(\alpha-\beta)-\sqrt{(\alpha-\beta)(\alpha-\gamma)}}\ (\beta - \alpha + \sqrt{(\alpha-\beta)(\alpha-\gamma)}) \\ &= (\alpha-\beta)\sqrt{\alpha-\gamma} - (\alpha-\gamma)\sqrt{\alpha-\beta}. \end{aligned}$$

Then $\sigma_1((\alpha-\beta)\sqrt{(\alpha-\gamma)} + (\alpha-\gamma)\sqrt{(\alpha-\beta)}) = (\alpha-\beta)\sqrt{(\alpha-\gamma)} - (\alpha-\gamma)\sqrt{(\alpha-\beta)}$ and we get the conditions

**3)** $\sigma_1(\sqrt{\alpha-\gamma}) = \sqrt{\alpha-\gamma}$,

**4)** $\sigma_1(\sqrt{\alpha-\beta}) = -\sqrt{\alpha-\beta}$.

Now, we require that the two columns of $\sigma_2$ are $\sigma_2(A')$ and $\sigma_2(B')$, i.e.

*iii*) $\sigma_2(A') = A' + 2B' = A' + B$,

*iv*) $\sigma_2(B') = 2A' - B' = A - B'$.

We consider *iii*). Since $2B = 0$, we have $B = -B$ and then $A' + B = -(-A' - B) = -(-A' + B)$. Therefore the point $A' + B$ is the opposite of the point $B - A'$, that we have already calculated. Thus the two points have the same abscissas and opposite ordinates. We get the following conditions:

**5)** $\sigma_2(\sqrt{\alpha - \gamma}) = -\sqrt{\alpha - \gamma}$,

**6)** $\sigma_2(\sqrt{\alpha - \beta}) = \sqrt{\alpha - \beta}$.

Now, we consider *iv*). We calculate $A - B'$:

$$\lambda_{A-B'} = \frac{-(\beta-\gamma)\sqrt{\beta-\alpha}-(\beta-\alpha)\sqrt{\beta-\gamma}}{\beta-\alpha+\sqrt{(\beta-\alpha)(\beta-\gamma)}} = -\frac{(\beta-\gamma)\sqrt{\beta-\alpha}+(\beta-\alpha)\sqrt{\beta-\gamma}}{\beta-\alpha+\sqrt{(\beta-\alpha)(\beta-\gamma)}},$$

$$\lambda^2_{A-B'} = \frac{(\beta-\gamma)^2(\beta-\alpha)+(\beta-\gamma)(\beta-\alpha)^2+2(\beta-\alpha)(\beta-\gamma)\sqrt{(\beta-\alpha)(\beta-\gamma)}}{(\beta-\alpha)^2+(\beta-\alpha)(\beta-\gamma)+2(\beta-\alpha)\sqrt{(\beta-\alpha)(\beta-\gamma)}} = \beta - \gamma,$$

$$\begin{aligned} x_{A-B'} &= \lambda^2_{A-B'} - x_A - x_{B'} = \beta - \gamma - \alpha - \beta - \sqrt{(\beta-\alpha)(\beta-\gamma)} \\ &= \beta - \sqrt{(\beta-\alpha)(\beta-\gamma)}. \end{aligned}$$

$$\begin{aligned} y_{A-B'} &= \lambda_{A-B'}(x_A - x_{A-B'}) - y_A \\ &= -\frac{(\beta-\gamma)\sqrt{\beta-\alpha}+(\beta-\alpha)\sqrt{\beta-\gamma}}{(\beta-\alpha)+\sqrt{(\beta-\alpha)(\beta-\gamma)}}\ (\alpha - \beta + \sqrt{(\beta-\alpha)(\beta-\gamma)}) \\ &= (\beta-\alpha)\sqrt{\beta-\gamma} - (\beta-\gamma)\sqrt{\beta-\alpha}. \end{aligned}$$

Then $y_{\sigma_2(B')} = y_{A-B'}$ implies

**7)** $\sigma_2(\sqrt{\beta - \gamma}) = \sqrt{\beta - \gamma}$,

**8)** $\sigma_2(\sqrt{\beta - \alpha}) = -\sqrt{\beta - \alpha}$.

To get all the conditions for $\alpha, \beta$, and $\gamma$, we finally require that the two columns of $\sigma_3$ are $\sigma_3(A')$ and $\sigma_3(B')$, i.e.

*v*) $\sigma_3(A') = A' + B$,

*vi*) $\sigma_3(B') = B'$.

The condition *v*) for $\sigma_3$ is the same of the condition *iii*) for $\sigma_2$. Thus we have

**9)** $\sigma_3(\sqrt{\alpha-\gamma}) = -\sqrt{\alpha-\gamma}$,

**10)** $\sigma_3(\sqrt{\alpha-\beta}) = \sqrt{\alpha-\beta}$.

Now we consider *vi*). Clearly we have

**11)** $\sigma_3(\sqrt{\beta-\gamma}) = \sqrt{\beta-\gamma}$,

**12)** $\sigma_3(\sqrt{\beta-\alpha}) = \sqrt{\beta-\alpha}$.

We resume all the found conditions:

**1)** $\sigma_1(\sqrt{\beta-\alpha}) = -\sqrt{\beta-\alpha}$,

**2)** $\sigma_1(\sqrt{\beta-\gamma}) = -\sqrt{\beta-\gamma}$,

**3)** $\sigma_1(\sqrt{\alpha-\gamma}) = \sqrt{\alpha-\gamma}$,

**4)** $\sigma_1(\sqrt{\alpha-\beta}) = -\sqrt{\alpha-\beta}$,

**5)** $\sigma_2(\sqrt{\alpha-\gamma}) = -\sqrt{\alpha-\gamma}$,

**6)** $\sigma_2(\sqrt{\alpha-\beta}) = \sqrt{\alpha-\beta}$,

**7)** $\sigma_2(\sqrt{\beta-\gamma}) = \sqrt{\beta-\gamma}$,

**8)** $\sigma_2(\sqrt{\beta-\alpha}) = -\sqrt{\beta-\alpha}$,

**9)** $\sigma_3(\sqrt{\alpha-\gamma}) = -\sqrt{\alpha-\gamma}$,

**10)** $\sigma_3(\sqrt{\alpha-\beta}) = \sqrt{\alpha-\beta}$,

**11)** $\sigma_3(\sqrt{\beta-\gamma}) = \sqrt{\beta-\gamma}$,

**12)** $\sigma_3(\sqrt{\beta-\alpha}) = \sqrt{\beta-\alpha}$.

We observe that 2) together with 4) imply

$$\sigma_1(\sqrt{(\alpha-\beta)(\beta-\gamma)}) = \sigma_1(\sqrt{\alpha-\beta})\sigma_1(\sqrt{\beta-\gamma}) = (-\sqrt{\alpha-\beta})(-\sqrt{\beta-\gamma})$$

$$= \sqrt{\alpha-\beta}\sqrt{\beta-\gamma} = \sqrt{(\alpha-\beta)(\beta-\gamma)}$$

Then $\sigma_1$ fixes $\sqrt{(\alpha-\beta)(\beta-\gamma)}$. By using 6) together with 7) and 10) together with 11) in the same way, we may observe that $\sigma_2$ and $\sigma_3$ also fix $\sqrt{(\alpha-\beta)(\beta-\gamma)}$. Then $(\alpha-\beta)(\beta-\gamma)$ has to be a rational square. On the contrary, the condition 2), the condition 4) and the condition 5) respectively imply that $\beta-\gamma$, $\alpha-\beta$ and $\alpha-\gamma$ are not rational squares.

Then $G$ is the Galois group $\mathrm{Gal}(\mathbb{Q}(\mathcal{E}[4])/\mathbb{Q})$ if and only if $(\alpha-\beta)(\beta-\gamma)$ is a rational square and $\mathbb{Q}(\sqrt{-1}, \sqrt{\alpha-\beta}, \sqrt{\beta-\gamma}, \sqrt{\alpha-\gamma})$ has degree 8 over $\mathbb{Q}$.

Furthermore, by using the conditions 6), 7), 10) and 11), we have that the fixed field of the group $< \sigma_2, \sigma_3 >$ is $K_0 = \mathbb{Q}(\sqrt{\alpha-\beta}, \sqrt{\beta-\gamma})$. Since we are requiring that $\sqrt{\alpha-\beta}$ and $\sqrt{\beta-\gamma}$ are not rational numbers, but $(\alpha-\beta)(\beta-\gamma)$ is a rational square, we have that the field $K_0$ has degree 2 over $\mathbb{Q}$ as desired.

# Appendix B

# Direct computation when $q = 2^2$ Part two

We show by direct computation that the point $P$ found in 2.1, for the cases when $|G| = 8$, is not divisible by 4 over $\mathbb{Q}$.

## B.1 Global divisibility by 4 does not hold for $P$

We consider the elliptic curve

$$\mathcal{E}: \quad y^2 = x(x+93)(x-31)(x-62) = x^3 - 6727x + 178746$$

and its points

$$D = \left(-\frac{403}{2} - \frac{31}{2}\sqrt{-31}, 1922 - 434\sqrt{-31}\right) \quad \text{and} \quad P = 4D = \left(\frac{5006244481}{16646400}, -\frac{341996266999871}{67917312000}\right)$$

found in 2.1, in the case when $|G| = 8$. The abscissas of the 16 points $D^*$ such that $4D^* = P$ are the roots of the polynomials:

$$f_1 = 289x^4 - 31992x^3 + 3888206x^2 - 198050568x + 7359538849,$$

$$f_2 = 225x^4 - 59644x^3 + 3027150x^2 + 79482388x - 479307399,$$

$$f_3 = 16x^4 + 4991x^3 + 215264x^2 - 56453945x + 1616161750,$$

$$f_4 = x^4 - 4748x^3 + 13454x^2 + 30509828x - 803433479.$$

We want to verify that they are not rational numbers. The roots of the polynomial $f_1$ are

$$x_{1,1} = \frac{(248\sqrt{-1}+465)\sqrt{155}+18600\sqrt{-1}+7998}{289}$$

$$x_{1,2} = \frac{(248\sqrt{-1}-465)\sqrt{155}-18600\sqrt{-1}+7998}{289}$$

$$x_{1,3} = -\frac{(248\sqrt{-1}-465)\sqrt{155}+18600\sqrt{-1}-7998}{289}$$

$$x_{1,4} = -\frac{(248\sqrt{-1}+465)\sqrt{155}-18600\sqrt{-1}-7998}{289},$$

then they lie in $\mathbb{Q}(\sqrt{-1},\sqrt{155})$. The roots of the polynomial $f_2$ are

$$x_{2,1} = \frac{62\sqrt{-31}+1271}{9} \qquad x_{2,2} = -\frac{62\sqrt{-31}-1271}{9}$$

$$x_{2,3} = \frac{62\sqrt{-31}-217}{25} \qquad x_{2,4} = -\frac{62\sqrt{-31}+217}{25},$$

then they lie in $\mathbb{Q}(\sqrt{-31})$. The roots of the polynomial $f_3$ are

$$x_{3,1} = \frac{31\sqrt{31}-403}{2} \qquad x_{3,2} = -\frac{31\sqrt{31}+403}{2}$$

$$x_{3,3} = \frac{31\sqrt{31}+1457}{32} \qquad x_{3,4} = -\frac{31\sqrt{31}-1457}{32},$$

then they lie in $\mathbb{Q}(\sqrt{31})$. Finally, the roots of the polynomial $f_4$ are

$$x_{4,1} = 1054\sqrt{5}+2387 \qquad x_{4,2} = -1054\sqrt{5}+2387$$

$$x_{4,3} = 34\sqrt{5}-13 \qquad x_{4,4} = -34\sqrt{5}-13,$$

then they lie in $\mathbb{Q}(\sqrt{5})$. We have verified that $P$ is not divisible by 4 over $\mathbb{Q}$.

# Appendix C

# Direct computation when $q = 3^2$

In section 4.2 we have found a point $P$ on the elliptic curve $y^2 = x^3 + 16$, that gives a negative answer to the Local-Global Divisibility Problem when $q = 9$ on the field $L = \mathbb{Q}(\sqrt{17}, \zeta_3)$. Now, we will show how it is possible to prove by direct computation, that this point is not globally divisible by 9 over $L$.

## C.1 Global divisibility by 9 does not hold for $P$

We evaluate the polynomial 4.1.1 in $k = 1$ and we find

$$x_{3Q} = \frac{x^9 - 1536x^6 + 12288x^3 + 262144}{9x^8 + 1152x^5 + 36864x^2}$$

The abscissas of the 3-divisors of $P$ are the roots $a_1$, $a_2$, ..., $a_9$ of the polynomial $q := x_{3Q} - u_9$. The factorization of $q$ over $L$ is

$$\frac{1}{9} \cdot (x + \frac{(127h - 3903)\zeta_3 - 127h + 4479}{4225}) \cdot (x + \frac{(-127h + 4479)\zeta_3 + 127h - 3903}{4225})$$

$$\cdot (x + \frac{(-381h - 7159)\zeta_3 - 381h - 7159}{2809}) \cdot (x + \frac{(381h - 32305)\zeta_3 + 381h - 32305}{2809})$$

$$\cdot (x + \frac{(-2204085h + 115931205)\,\zeta_3 - 1554861h + 144935761}{26512201}) \cdot (x + \frac{-65\zeta_3 - 65}{3})$$

$$\cdot (x + \frac{(2204085h - 29538405)\,\zeta_3 + 1554861h + 42314935}{26512201})$$

$$\cdot (x + \frac{(-1554861h + 144935761)\,\zeta_3 - 2204085h + 115931205}{26512201})$$

$$\cdot (x + \frac{(1554861h + 42314935)\,\zeta_3 + 2204085h - 29538405}{26512201})$$

Therefore $a_i \in L$ for $i = 1, 2, ..., 9$. It is possible to verify that the ordinates corresponding to those abscissas are in $L$ too. The abscissas of the 9-divisors of $P$ are the roots $a_{i,j}$, $i, j \in \{1, 2, ..., 9\}$, of the numerators $s_i$ of the polynomials $qi := x_{3Q} - a_i$. This polynomials are

$$\begin{aligned}
s_1 =& \frac{1}{9}x^9 + \frac{(-381h-7159)\zeta_3 - 381h - 7159}{2809}x^8 - \frac{512}{3}x^6 \\
&+ \frac{(-48768h-916352)\zeta_3 - 48768h - 916352}{2809}x^5 + \frac{4096}{3}x^3 \\
&+ \frac{(-1560576h-29323264)\zeta_3 - 1560576h - 29323264}{2809}x^2 - \frac{262144}{9}
\end{aligned}$$

$$\begin{aligned}
s_2 =& \frac{1}{9}x^9 + \frac{(-2204085h+115931205)\zeta_3 - 1554861h + 144935761}{26512201}x^8 - \frac{512}{3}x^6 + \\
&+ \frac{(-282122880h+14839194240)\zeta_3 - 199022208h + 18551777408}{26512201}x^5 + \frac{4096}{3}x^3 \\
&+ \frac{-9027932160h+474854215680)\zeta_3 - 6368710656h + 93656877056}{26512201}x^2 - \frac{262144}{9}
\end{aligned}$$

$$\begin{aligned}
s_3 =& \frac{1}{9}x^9 + \frac{(-1554861h+144935761)\zeta_3 - 2204085h + 115931205}{26512201}x^8 - \frac{512}{3}x^6 \\
&+ \frac{(-199022208h+18551777408)\zeta_3 - 282122880h + 14839194240}{26512201}x^5 \ \frac{4096}{3}x^3 \\
&+ \frac{(-6368710656h+593656877056)\zeta_3 - 9027932160h + 474854215680}{26512201}x^2 - \frac{262144}{9}
\end{aligned}$$

$$\begin{aligned}
s_4 =& \frac{1}{9}x^9 + \frac{(-127h+4479)\zeta_3 + 127h - 3903}{4225}x^8 - \frac{512}{3}x^6 \\
&+ \frac{(-16256h+573312)\zeta_3 + 16256h - 499584}{4225}x^5 + \frac{4096}{3}x^3 \\
&+ \frac{(-520192h+18345984)\zeta_3 + 520192h - 15986688}{4225}x^2 - \frac{262144}{9}
\end{aligned}$$

$$\begin{aligned}
s_5 =& \frac{1}{9}x^9 + \frac{-65\zeta_3 - 65}{3}x^8 - \frac{512}{3}x^6 + \frac{-8320\zeta_3 - 8320}{3}x^5 + \frac{4096}{3}x^3 + \frac{-266240\zeta_3 - 266240}{3}x^2 \\
&- \frac{262144}{9}
\end{aligned}$$

$$
\begin{aligned}
s_6 =& \frac{1}{9}x^9+\frac{(127h-3903)\zeta_3-127h+4479}{4225}x^8-\frac{512}{3}x^6 \\
&+\frac{(16256h-499584)\zeta_3-16256h+573312}{4225}x^5+\ \frac{4096}{3}x^3 \\
&+\frac{(520192h-15986688)\zeta_3-520192h+18345984}{4225}x^2-\frac{262144}{9}
\end{aligned}
$$

$$
\begin{aligned}
s_7 =& \frac{1}{9}x^9+\frac{(1554861h+42314935)\zeta_3+2204085h-29538405}{26512201}x^8-\frac{512}{3}x^6 \\
&+\frac{(199022208h+5416311680)\zeta_3+282122880h-3780915840}{26512201}x^5+\ \frac{4096}{3}x^3 \\
&+\frac{(6368710656h+173321973760)\zeta_3+9027932160h-120989306880}{26512201}x^2-\frac{262144}{9}
\end{aligned}
$$

$$
\begin{aligned}
s_8 =& \frac{1}{9}x^9+\frac{(2204085h-29538405)\zeta_3+1554861h+42314935}{26512201}x^8-\frac{512}{3}x^6 \\
&+\frac{(282122880h-3780915840)\zeta_3+199022208h+5416311680}{26512201}x^5+\ \frac{4096}{3}x^3 \\
&+\frac{(9027932160h-120989306880)\zeta_3+6368710656h+173321973760}{26512201}x^2-\frac{262144}{9}
\end{aligned}
$$

$$
\begin{aligned}
s_9 =& \frac{1}{9}x^9+\frac{(381h-32305)\zeta_3+381h-32305}{2809}x^8-\frac{512}{3}x^6 \\
&+\frac{(48768h-4135040)\zeta_3+48768h-4135040}{2809}x^5+\ \frac{4096}{3}x^3 \\
&+\frac{(1560576h-132321280)\zeta_3+1560576h-132321280}{2809}x^2-\frac{262144}{9}
\end{aligned}
$$

By using the input "factor($s_i, [h, \zeta_3]$)" in Axiom, we can verify that $s_i$ does not split in linear factors over $L$, for all $i = 1, 2, ..., 9$. In particular, the polynomials $s_1, s_2, s_3, s_7, s_8$ and $s_9$ are irreducible over $L$ and the factorizations of the other three polynomials over that field are

$$
\begin{aligned}
s_4 =& \frac{1}{9}\cdot(x^3+\frac{(-69h+2133)\zeta_3-3h+1239}{169}x^2+64)\cdot(\frac{(3h+1041)\zeta_3+69h-2421}{169}x^2+64) \\
&\cdot(x_3+\frac{(3h-231)\zeta_3-3h-33}{25}x^2+64)
\end{aligned}
$$

$$s_5 = \frac{1}{9}\cdot(x^3 + ((-3h+3)\zeta_3 - 3h + 3)x^2 + 64) \cdot (x_3 + (-3\zeta_3 - 3)x^2 + 64)$$
$$\cdot(x_3 + ((3h - 195)\zeta_3 + 3h - 195)x^2 + 64)$$

$$s_6 = \frac{1}{9}\cdot(x^3 + \frac{(-3h-33)\zeta_3+3h-231}{25}x^2 + 64) \cdot (\frac{(-3h+1239)\zeta_3-69h+2133}{169}x^2 + 64)$$
$$\cdot(x_3 + \frac{(69h-2421)\zeta_3+3h+1041}{169}x^2 + 64)$$

# Bibliography


[AT] Artin E., Tate J., *Class field theory*, Benjamin, Reading, MA, 1967.

[Cas] Cassels J. W. S., *Quadratic Forms*, London Mathematical Society, Academic Press, 1978.

[Cas2] Cassels J. W. S., *Local Fields*, London Mathematical Society, 1986.

[DZ] Dvornicich R., Zannier U., *Local-global divisibility of rational points in some commutative algebraic groups*, Bull. Soc. Math. France, **129** (2001), 317-338.

[DZ2] Dvornicich R., Zannier U., *An analogue for elliptic curves of the Grunwald-Wang example*, C. R. Acad. Sci. Paris, Ser. I **338** (2004), 47-50.

[DZ3] Dvornicich R., Zannier U., *On local-global principle for the divisibility of a rational point by a positive integer*, Bull. Lon. Math. Soc., no. **39** (2007), 27-34.

[Gru] Grunwald W., *Ein allgemeines Existenztheorem für algebraische Zahlkörper*, Journ. f.d. reine u. angewandte Math., **169** (1933), 103-107.

[Ill] Illengo M., *Cohomology of integer matrices and local-global divisibility on the torus*, J. Théor. Nombres Bordeaux, **20** (2008), no. 2, 1-8, to appear.

[Kob] Koblitz N., *P-adic numbers, p-adic analysis, and zeta-functions*, Springer Verlag, 1979.

[Lan] Lang S. , *Algebra*, Addison-Wesley , 1993.

[Lan2] Lang S., *Number Theory III*, Encyclopaedia of Mathematical Sciences 60 (Springer, 1991).

[LT] Lang S., Tate J. *Principal homogeneous spaces over abelian variety*, American J. Math., no. **80** (1958), 659-684.

[Maz] Mazur B., *Rational isogenies of prime degree (with an appendix by D. Goldfeld)*, Invent Math., **44** (1978), no. 2, 129-162.

[Mer] Merel L., *The field generated by the points of small prime order on an elliptic curve*, Math. Res. Notices, no. **20** (2001), 1075-1082.

[Mer2] Merel L., *Sur la nature non-cyclotomique des points d'ordre fini des courbes elliptiques. (French) [On the noncyclotomic nature of finite-order points of elliptic curves] With an appendix by E. Kowalski and P. Michel*, Duke Math. J. **110** (2001), no. 1, 81-119.

[Neu] Neukirch J., *Algebraic Number Theory*, Springer.

[Reb] Rebolledo M., *Supersingular module, Gross-Kudla formula and rational points of modular curves*, Pacific J. Math., no. **234** (2008), no. 1, 167-184.

[San] Sansuc J.-J., *Groupe de Brauer et arithméthique des groupes linéaires sur un corps de nombres*, J. reine angew. Math., t. **327** (1981), 12-80.

[Ser] Serre J.-P. *Algebraic Groups and Class Field*, Springer Verlag, 1998.

[Ser2] Serre J.-P. *Topics in galois Theory*, Jones and Bartlett, Boston 1992.

[Sil] Silverman J. H., *The arithmetic of elliptic curves*, Springer.

[ST] Silverman J. H., Tate J., *Rational points on elliptic curves*, Springer.

[Tro] Trost E., *Zur theorie des Potenzreste*, Nieuw Archief voor Wiskunde, no. **18** (2) (1948), 58-61.

[Wan] Wang Sh., *A counter example to Grunwald's theorem*, Annals of Math., no. **49** (1948), 1008-1009.

[Wan2] Wang Sh., *On Grunwald's theorem*, Annals of Math., no. **51** (1950), 471-484.

[Wha] Whaples G., *Non-analytic class field theory and Grunwald's theorem* , Duke Math. J., no. **9** (1942), 455-473.

[Won] Wong S., *Power residues on abelian variety*, Manuscripta Math., no. **102** (2000), 129-137.